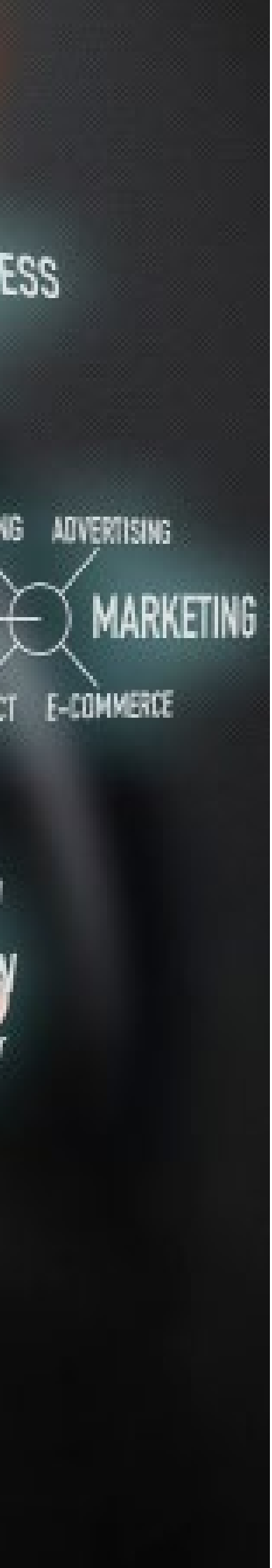
Deloitte.

On the horizon
2016 Hot topics for IT Internal Audit in African Financial Services

An Internal Audit viewpoint

#DeloitteRA


IDEA
CONCEPT
SPIRATION
RISK
FUTURE
SALES
TARGET
OBJECTIVES
SUCC
SOLUTION
SOCIAL MEDIA
BRANDI
BUSINESS
INTERNET
PRODU
MOTIVATION
EDUCATION
AGEMENT
VISIO
TEAMWORK
SYNERGY
PLANNING
RESEARCH
SUPPORT
DEVELOPMENT
ANALYSIS
PROCESS
STRATEGY



Introduction

Welcome to our first annual review of the information technology hot topics facing internal audit functions in African financial services. Our survey primarily focuses on the financial services sector for Southern and East Africa.

Executive management and internal audit departments in financial services continue to operate within an evolving environment of new regulatory requirements (e.g. Financial Crime), emerging risks (e.g. new technologies; mobile and digital) and expanding stakeholder expectations (drive for innovation). This environment is further challenged by the arrival of new entrants into the world of financial services that are likely to disrupt and transform the industry.

There are a number of core control areas that feature in the 2016 hot topics, such as traditional high-profile items, which form the backbone of IT internal audit plans.

Cyber security unsurprisingly features as one of the highest priority topics in countries such as South Africa and Kenya, which is aligned with what we are seeing globally. What is interesting to note is that even organisations with a relatively mature control environment, continue to see this as a key area of audit focus as they try to align their approach with the growing regulatory expectations on how to assure such a mutating global threat. This is exacerbated by ongoing internal challenges around information security, managing logical access of large volumes of users, over multiple systems and multiple business units in different geographic regions which continue to introduce vulnerabilities in the IT environment.

IT Disaster Recovery and Resilience continues to be a high priority for African banks and companies in the financial services sector, possibly fuelled by ongoing power challenges across the continent, coupled with the need for uninterrupted availability.

The exponential growth we are seeing on the African continent in the areas of mobile and digital escalates the risk associated with these technologies to a key agenda item for management and internal audit. Strategic or large-scale change was another key theme which reflects the regulatory focus and growing expectations by Boards on managing strategic initiatives and providing appropriate oversight over the associated execution risk across the organisation.

Organisations from Financial Services sectors across South Africa, Kenya, Tanzania and Uganda have participated in this survey; comparing and contrasting the key areas of focus of IT internal audit functions in each of the countries, it is not surprising to see that the core areas of resilience, cyber and digital risk feature consistently in the top 5 of organisations in all countries.

We ran a similar survey in the UK which found that participants from the retail banking, insurance and investment management sector underlined the challenges in auditing legacy infrastructure and systems, with retail banking particularly highlighting the recent changes in payment models. The UK banking sub-sector is facing challenges from emerging competition from new providers who are heavily investing in payment systems, while at the same time it grapples with high profile payment outages which threaten the availability of existing payment services.

The UK publication has been well received, both in the financial services sector and beyond, by Heads of IT Internal Audit and Heads of Audit as well as by IT Directors and IT Risk functions. We hope that our African insights in this sector will be useful and help IT Audit departments benchmark their own IT Audit plans for 2016.

Table 1
Africa – IT Internal Audit Hot Topics: 2016
The table below summarises the key IT Audit hot topics as identified by Heads of IT Audit and Heads of Internal Audit from 21 banks and financial service organisations across South and East Africa:

2016 IT Hot Topics				
Rank	**South Africa**	**Kenya**	**Tanzania**	**Uganda**
1	Disaster Recovery & Resilience	Cyber Security	Disaster Recovery & Resilience	Information Security
2	Cyber Security	IT Governance & IT Risk Management	Digital & Mobile Risk	Digital & Mobile Risk
3	Information Security	Digital & Mobile Risk	Information Security	Data Management & Governance
4	IT Governance & IT Risk Management	Disaster Recovery & Resilience	Cyber Security	IT Governance & IT Risk Management
5	Digital & Mobile Risk	Information Security	Large Scale Change	Enterprise Technology Architecture
6	Large Scale Change	Data Management & Governance	Data Management & Governance	Cloud Outsourcing
7	Enterprise Technology Architecture	Large Scale Change	IT Governance & IT Risk Management	Third Party Management
8	Data Management & Governance	Service Management	Enterprise Technology Architecture	Disaster Recovery & Resilience
9	Cloud Outsourcing	Enterprise Technology Architecture	Cloud Outsourcing	Large Scale Change
10	Service Management	Cloud Outsourcing	Third-Party Management	Service Management
11	Third Party Management	Third Party Management	Service Management	Cyber Security

■ Top 5 overall or common areas across all countries covered

Table 2
United Kingdom IT Internal Audit Hot Topics: 2012 – 2016

As a comparative, we have included the table below which compares the top 10 IT internal audit hot topics over the past five years as identified through our annual UK survey of internal audit functions in the Financial Services industry. It highlights some interesting trends over time. The table also confirms the core, high-profile topics that have appeared consistently in the Top 10 of internal audit functions (which are marked in bold).

Top 10	2016	2015	2014	2013	2012
1	**Cyber Security**	**Cyber Security**	Large Scale Change	**Third Party Management**	**Cyber Threat**
2	Strategic Change	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Identity and Access Management	Complex Financial Models
3	**Third Party Management**	Large Scale Change	Identity & Access Management and Data Security	**Data Governance and Quality**	Data Leakage
4	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	**Data Governance & Quality**	Large Scale Change	**Data Governance and Data Quality**
5	**Data Management and Data Governance**	**Third Party Management**	**Third Party Management**	**Cyber Security**	Rogue Trader and Access Segregation
6	Information Security	Information Security	**Cyber Security**	**Resilience**	Regulatory Programmes
7	Digital Risk	Digital and Mobile Risk	Digital Risk	Cloud Computing	Financial Crime
8	IT Governance and IT Risk Management	**Data Management and Governance**	Service Management	Mobile Devices	**Third Party Management**
9	Enterprise Technology Architecture	IT Governance and IT Risk Management	**Disaster Recovery and Resilience**	Complex Financial Modelling	Social Media
10	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

Topics, which appear in more than two years, have been colour-coded to help illustrate their movement in the top 10 over time.

Top 10 hot topics across Africa

1. Disaster Recovery and Resilience

IT system failures are front page news, leading to public coverage and reputational damage for a number of financial institutions. Outages impacting ATM networks, digital services, payment systems, and ultimately customer access to services continue to focus the attention of regulators and drive organisations to place added focus on the stability of their systems. The effect and impact of planned power supply disruptions also factors into the resiliency capabilities of the aforementioned services. As a result, IT disaster recovery and resilience remains a key area of focus for Heads of IT Internal Audit.

Many progressive institutions are moving their focus from a traditional IT disaster recovery and resilience plan to better understand the risks to services inherent in their IT environments, both in-house and outsourced services, and the controls to mitigate these risks. IT failures rarely result in a full invocation of the disaster recovery and resilience plan for IT as they are more often than not the result of a management process issue or human error, rather than a "big ticket" data centre outage. With this in mind, it is imperative that internal audit functions broaden their focus to determine the adequacy of processes in place to avoid, respond, recover and learn from planned and unplanned outages. While technology is at the heart of the disaster recovery, resilience, in line with regulatory expectations, should be broader, encompassing areas such as operations, information and corporate security, communications, public relations and crisis management.

2. Cyber Security

It is no surprise that Cyber appears as one of the top concerns for IT internal audit professionals in the industry. Indeed it has been an increasingly regular feature in the media over the past 18 months, with multiple significant attacks and data breaches impacting all countries, including some high-profile incidents for financial services firms. The cost of Cyber-crime in 2014 has been estimated at 0.41% of Gross Domestic Profit (GDP) within the European Union and 0.14% within South Africa.

Cyber security is not simply about fixing the vulnerability that was exploited, but wider crisis management skills, including public, media and customer relations. With the increase in breach impact and complexity in 2015, incident response has seen a shift from a point-based 'fix-it' type approach towards more robust enterprise assessments of cyber risk with internal controls around incident response. This has also driven a need for businesses to systematically understand cyber risk at the Board level.

Internal audit functions have an opportunity to demonstrate that they can understand and provide assurance over all the above. They can help to promote more organisational collaboration in Cyber audits, both internally (across functions) and externally, as this will be a key area of focus for the sector over coming months. This should enable a more transparent view of emerging risks and threats, and in turn drive more effective risk management practices while allowing internal audit to remain agile to the changing nature of Cyber threats. For the organisations with a less mature Cyber control environment, Heads of IT Audit understandably see Cyber as a topic of focus and concern in light of their organisation's legacy control weaknesses; however, even the more mature organisations are still concerned about keeping up with growing regulatory expectations on "what good looks like" and how to provide commensurate levels of assurance over Cyber.

3. Digital and Mobile Risk

Digital channels such as mobile, cloud and social media are interacting and converging. While this convergence holds the promise of new opportunities for organisations, digital also introduces new risks that may not be effectively managed by the organisations' existing governance, oversight and internal controls frameworks. A number of these risks were noted in the UK Financial Conduct Authority's (FCA) thematic review on mobile banking[1], where financial institutions are using mobile banking as a catalyst for enhancing existing frameworks and future-proofing their digital risk landscape by having a better understanding of their digital footprint.

Usage of mobile devices to carry out traditional banking functions is growing in South and East Africa, in part due to the penetration of internet usage via smartphone devices combined with the focus on mobile and app based banking and payment services being driven by the financial services sector.

Identifying, mapping and truly understanding the organisation's digital footprint will help internal audit functions to have a more targeted and risk focused view of the firm's digital landscape, which in turn can lead to a structured and robust plan for effective auditing of 'digital' and unearthing the associated residual risk. The role of Internal Audit in this era of fast-moving digital innovation and transformation cannot be underestimated in providing genuine input, oversight and challenge to the digital parts of the business.

[1] FCA Thematic Review: TR14/15 Mobile Banking and Payments (September 2014)

4. Information Security

For some organisations, the topic of cyber is considered to include aspects of business continuity, crisis management, financial crime and fraud as well as traditional information security. For others, information security remains a topic of importance in its own right, which warrants its own place in the internal audit plan. Either way, the emergence of cyber in the past few years has shone a spotlight on the need to 'fix the basics' in order to minimise exposure to cyber threats. In many cases in financial services, fixing the basics is about assuring the appropriateness of access to information and focusing on identity and access management initiatives.

High-profile data loss incidents continue to make headlines, irk regulators and generate considerable workload across the three lines of defence to ensure that access is managed effectively. Given the scale of many financial services organisations, along with the size of their IT estates, this is a vast and continual challenge. We note in particular several banks with extensive 'Privileged Access Management' programmes aiming to minimise the volume of accounts with privileged access to systems along with similar programmes to sever direct access to systems by third-party organisations. Internal audit functions are providing assurance over the effectiveness of these programmes, conducting re-performance or verification exercises to confirm that access is appropriate once the remediation programmes have concluded.

Within the European Union, data suggests the agreement on the General Data Protection Regulation (GDPR) will be reached by the end of 2015. GDPR seeks to unify data protection within the European Union with a single law. In comparison, the implementation of and adherence to the POPI (Protection of Personal Information) act by financial institutions, banks and third party service providers within the South African region serves to achieve many of the same outputs. We note specifically, Condition 7 of the Act, "Data Safeguards" which prescribes security measures on integrity and confidentiality of personal information.

5. IT Governance and IT Risk Management

We have seen a significant uptake of IT governance and risk audits in the past 18 months and an increased emphasis on providing a view on whether the "information technology governance of the organisation supports the organisation's strategies and objectives" in line with the Institute of Internal Auditors (IIA) code. Many IT governance assessments are structured in line with COBIT 5 and the recently revised ISO/IEC 38500:2015 framework. Internal audit functions are being challenged by their Boards and regulators to form an opinion regarding the transparency of decision-making and effectiveness of governance practices in their Technology teams, including the alignment of Technology with business strategy, the appropriateness of risk reporting to executive management and the Board, as well as the efficiency of mechanisms to measure performance.

A key component of this landscape is IT risk management, which covers Technology functions' compliance with not only enterprise-wide risk management requirements but also their approach towards identifying and managing technology risk proactively. It is becoming increasingly common for internal audit functions to include such aspects in their IT governance and risk assessments. We have also noted a shift by internal audit functions to auditing risk culture on a more granular level, through audits of Technology risk culture for instance. Such assessments are becoming an established measure for assessing the quality and embedding of an organisation's strategic plan, risk appetite, governance structure and its risk management frameworks. To meet the above challenges, internal audit departments should continue to ensure that they upskill their teams with subject matter expertise and experience in order to meet the expectation of their Boards and regulators.

6. Large Scale Change

There is a significant amount of change in support of organisational strategy across the organisations we surveyed. Whether this has been investment in new channels such as mobile, new products or business lines, acquisition or divestment or to reduce operational risks and "keep the lights on", technology is often at the heart of enabling these strategic changes. Internal audit functions are continuing to immerse themselves in the change portfolios and increase the resources allocated to assuring the strategic change programmes that the organisation is trying to deliver. It is becoming more typical for internal audit functions to include dedicated change audit teams and resources, with experience of technology development, change and testing as well as business change and project and programme delivery.

The challenge is how to deploy these resources effectively across the organisations' change portfolio and ensure that audit interventions are timely and provide a high impact on control improvement, without hindering the programme resources trying to deliver. In our experience, internal audit functions are

continuing to attend steering committees for a number of regulatory programmes (such as IFRS 9, BCBS 239, etc.) and the enormous change driven by Structural Reform in the Banking sector, providing assurance that these programmes are on track and are delivering their intended outcomes.

7. Enterprise Technology Architecture

Financial services organisations within the South African region remain heavily reliant on legacy estates with infrastructure and applications not suitably scalable, at an enterprise level to compete with the growing trends such as "big data", "single customer view", third party aggregation, or digital banking which now trend towards mobile customer interaction and changeability at a scale not catered for by legacy systems.

An initiative prevalent within the South African financial services industry during the 2014/2015 period was the transition away from legacy mainframe architecture, service virtualisation and the move to cloud computing. There are often large-scale transformation programmes in place to address these legacy issues. Internal audit functions are continuing to devote time to reviewing these programmes as well as the capability, functionality, resilience and security of the legacy systems, themselves.

The challenge for internal audit functions is, at one end of the spectrum, to retain the skills needed to test legacy platform controls, while the other end is to challenge the newer FinTech developments that are emerging and in some cases replacing the legacy estate.

8. Data Management and Data Governance

The volume of enterprise data is increasing exponentially, with more than 90% of the world's data estimated to have been created in the last two years alone[2]. Data governance brings benefits such as greater efficiency, visibility and cost savings, while in many cases helping to drive improvements in areas like data quality, or give greater confidence over data security. There has been a growing regulatory pressure to improve data governance, particularly in support of initiatives such as Anti-money Laundering and Basel III. In our experience, the most advanced organisations have addressed data governance at a senior level, with defined structures, policies and standards implemented across the entire organisation. This usually also involves the appointment of a Chief Data Officer (CDO).

Unfortunately, data governance implementations can be prone to becoming a leviathan of 'red tape' and onerous controls that do little to add value. Internal audit functions will naturally have assessed aspects of data control in previous audit plans, however as businesses increase their focus on the customer, digital channels and explicit requirements in regulations, the need to audit data governance practices more thematically is pressing. They will need to determine the scope of the governance activities to audit, and the depth of that assessment. Plans may need to extend over a timeline of several years, with a prioritised approach to address more business critical areas first.

For a large number of functions, auditing data governance requires expertise and toolsets, which may not have traditionally been contained within the function and therefore a level of upskilling may be required. Leading internal audit functions in financial services, however, far from continuing a perennial deferral of their data governance review, have taken the initiative through leveraging analytics capabilities which allow the use of sophisticated data quality and profiling tools to assess data quality comprehensively, and are actively helping to make sense of their organisation's data and unlock its value.

9. Cloud

The financial services sector is still in the early stages of adoption of cloud services, utilising combinations of public and private cloud offerings combined with in-house infrastructure to facilitate Customer Relationship Management (CRM), Application Development and Email as the most prevalent early adoptions. The adoption of cloud computing is noted to be lacking a defined and concerted strategy in terms of implementation and how to accommodate security and data protection requirements along with industry regulations. This topic has been prevalent in responses garnered from stakeholders surveyed within the South African region. Understanding how to ensure the security of customer data is another key element that requires engagement between cloud services providers and financial services firms in order to establish reusable frameworks for implementation.

Internal Audit functions can assist in this journey by ensuring they understand the organisation's current cloud footprint, conduct cloud audits starting at the procurement stage/process, and recognise the conditions that may prompt business users to bypass the IT shop and sign up for cloud services directly. They should also develop and leverage a customised framework tool to help identify the organisation's top cloud risks and drill down to key processes and controls.

[2] SINTEF. "Big Data, for better or worse: 90% of world's data generated over last two years." ScienceDaily

10. Third Party Management

Our survey highlighted that the management of third parties remains a key priority. Global third party ecosystems of organisations, also known as the 'extended enterprise', are becoming stronger sources of strategic advantage and the scale on which this is now taking place in financial services has increased. Businesses are also facing new risks, such as the threat of high profile business failure, accountability for illegal third party action or regulatory enforcement action with punitive fines, all leading to reputational damage and erosion of shareholder wealth. The Financial Services sector has dominated industry-specific regulation impacting the use of third parties; and this is expected to get even more severe. Deloitte estimates that the failure by large multinational businesses to appropriately identify and manage third parties, aside from the significant reputational damage, can lead to fines, direct compensation costs or other revenue losses in the range of US$ 2 – 50 million, while action under global legislation can be far higher, touching US$ 0.5 – 1 billion[3].

Internal Audit's focus on third party risk has traditionally been reactive and this decentralised approach to risk has led to micro-focus on risk areas aligned to certain parts of a business or functional areas for example, operational performance from an extended enterprise perspective or information security from a corporate security perspective. Internal audit functions should start to consider operational risk factors (e.g. performance, quality standards, delivery times, KPI/SLA measurement) with reputational and financial risk factors (e.g. an understanding of financial health, appropriate charging mechanisms and adherence to these) and legal and regulatory risks (e.g. compliance with anti-bribery regulations and awareness of global industry standards as they apply to third parties). An additional topic outside of the African Top 10, but a key global trend that warrants consideration is Payment Systems. The entrance of traditionally "non-financial" companies into the financial services sector as payment providers and aggregators, factor significantly into this topic.

11. Payment Systems

Recent developments from both a regulatory and technology perspective are causing a significant shift in traditional payment models, resulting in major changes in the market. This is providing a difficult set of challenges across the FS sector as banks face disruption from FinTech providers who are heavily investing in payment solutions. Cash is becoming increasingly replaced by contactless and mobile transactions as MPesa, Zapper, Hello Paisa, Instant Money and other offerings start to take a significant foothold in the market. High-profile payment outages are still all too common as institutions grapple with these future challenges while trying to ensure the 24/7 availability of existing payment services, often supported by legacy applications and infrastructure.

Internal audit functions need to upskill quickly and become more involved as organisations value their independent assurance on whether they are reacting appropriately to the risks related to the major regulatory and technological advances, and that existing systems are scalable with expected market changes. This includes regulatory risk assessments, security assessments, review of key payment projects and assessment of existing payment services to ensure appropriate current and future operability.

[3] Third Party Governance and Risk Management: Turning risk into opportunity; Deloitte Touche Tohmatsu Limited, 2015

Contacts

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 (0)83 304 4225
Email: navising@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader: Governance, Reguatory & Risk
Mobile: +27 (0)82 415 8253
Email: dechivers@deloitte.co.za

Graham Dawes
Chief Operating Officer: Risk Advisory East, West & Central Africa
Mobile: +254 719 892 209
Email: grdawes@deloitte.co.ke

Derek Schraader
Risk Advisory Africa Leader: Cyber Risk Services
Mobile: +27 (0)79 499 9046
Email: dschraader@deloitte.co.za

Shahil Kanjee
Risk Advisory Africa Leader: Technology Assurance & Advisory
Mobile: +27 (0)83 634 4445
Email: skanjee@deloitte.co.za

Werner Swanepoel
Risk Advisory Africa Leader: Data Analytics
Mobile: +27 (0)82 442 5948
Email: wswanepoel@deloitte.co.za

Michele Townsend
Director: Risk Advisory Southern Africa
Mobile: +27 (0)82 441 7164
Email: mntownsend@deloitte.co.za

Julie Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 720 111 888
Email: julnyangaya@deloitte.com

Designed and produced by Creative Services at Deloitte, Johannesburg. (000000/mar)