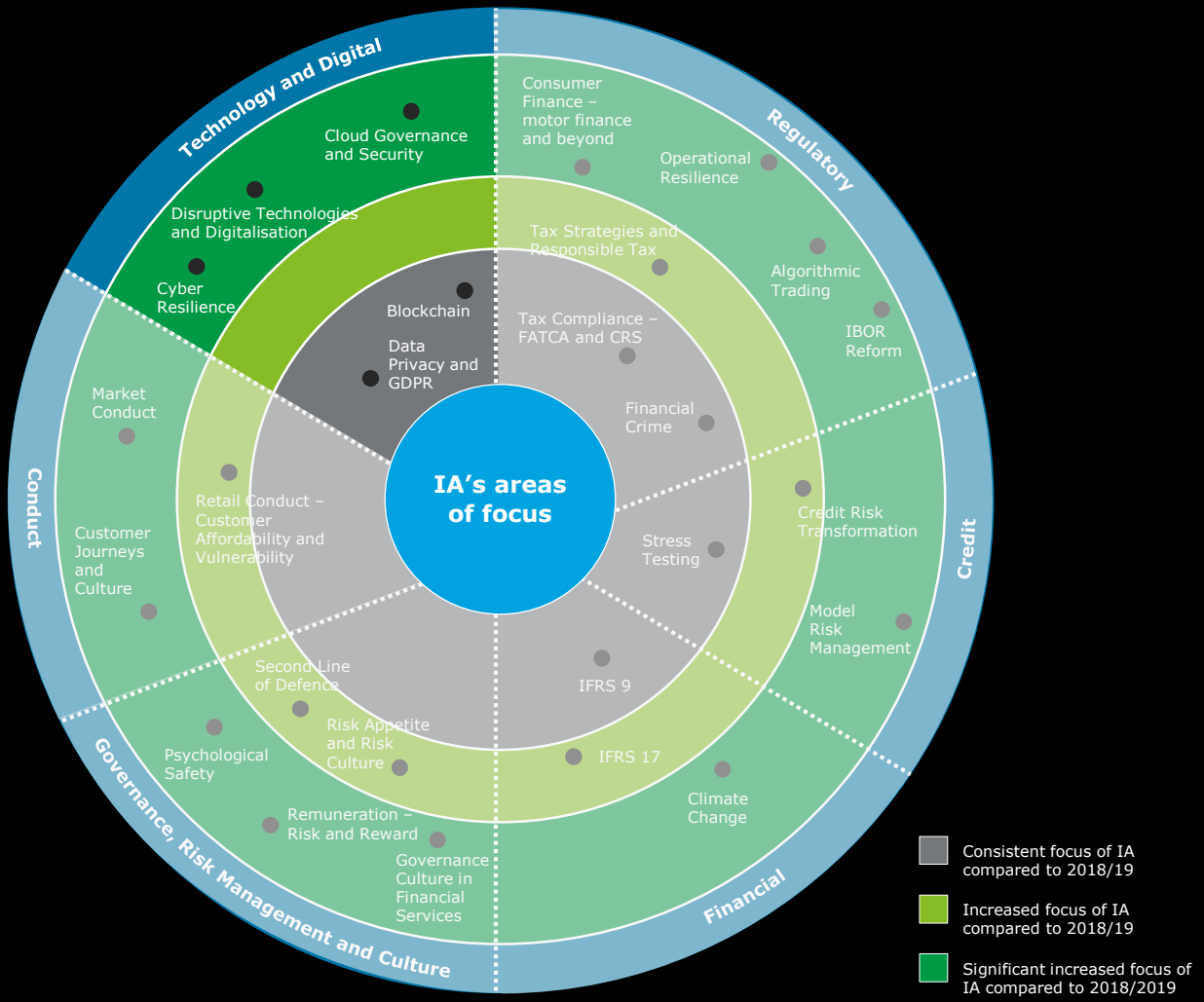
Deloitte.

Financial Services Internal Audit

Planning Priorities 2020 – Technology and Digital Hot Topics

Introduction

The industry is moving forward with large technology and digital enhancements including cyber resilience, disruptive technologies and digitalisation, blockchain and cloud. A number of costly technology and digital issues have arisen across financial services. Consequently, technology and digital risk are a significant priority for the industry and its regulators.



Contents

Key Industry Icons

Banking and Capital Markets

Insurance

Investment and Private Equity

6.1 Cyber Resilience

Why is it important?

Given the high profile cyber incidents across financial services in recent years, coupled with the continuing regulatory interest in this area – from the 'Dear Chairman Exercises (DCE) focusing on firms' technology resilience (DCE I and DCE II), to the Financial Policy Committee's (FPC) cyber stress testing pilot – it is expected that demands and requirements for organisations around cyber security and resilience will increase.

What's new?

The Bank of England, PRA and FCA issued a joint Discussion Paper, '*Building the UK financial sector's operational resilience*' in 2018 (DP 1/18), returning the spotlight to operational and cyber resilience.

This time the focus of the regulators is on the development of a broader framework for firms, enhancing resilience stress testing and establishing strong impact tolerances and performance metrics.

Financial services' organisations will be expected to set their own resilience tolerances (maximum downtime for instance), in line with a resilience baseline and take into account inter-connectedness with other financial services' firms.

What should Internal Audit be doing?

Area of focus	Description
Internal Audit's role	Internal Audit's role over the past few years has been critical in terms of applying a risk lens to the organisations' cyber agenda, driven by regulatory, senior management and board demands on assurance and challenge.
Areas of focus for the audit plan	Whilst this is not a new topic, Internal Audit functions cannot be complacent and should strive to raise the bar in line with broader developments. Areas of focus for Internal Audit functions to consider are: • The robustness of governance and senior manager accountability on cyber security. • The incident identification and response capability. • The development and implementation of a holistic, enterprise-wide approach for cyber and operational resilience, that can influence a 'resilience' culture in the organisation and drive resilience-by-design, particularly when it comes to the technology environment. • The data-based metrics to monitor disruption and performance against key indicators and tolerances by system/component, that can drive enhanced executive and board-level visibility and decision-making.

6.1 Cyber Resilience

Are there any potential challenges?

Challenge	Description
Audit timings and Board Audit Committee expectations	Many cyber initiatives and programmes have an objective of improving cyber maturity over a period of years. This makes determining the appropriate time to perform an audit challenging. Internal audit should not lose sight of their mandate and remit, and focus on their responsibility to provide the Board and Audit Committee with timely insight into the appropriateness of the organisation's approach to, and execution of, their cyber strategy on a regular (we suggest at least annual) basis.
Resources	The right skills are not always easy to find (and retain), particularly 'polymaths' with strong and deep IT expertise coupled with good business awareness. Organisations find it increasingly difficult to find and retain people that optimally combine cyber, technology and business audit skillsets, with the right interpersonal and softer skills to continue to drive together business and IT audit for truly integrated approaches that add value.

What Internal Audit skills are required?

Executives need to anticipate what the supervisory developments mean for their organisation and make decisions based on these, alongside their own threat analysis and cyber programmes. Equally, IT Internal Audit functions need to stay close to these developments and have a clear plan on what to do next. This, in turn, will inform the requisite skills and resource mix needed for the internal audit teams.

What's next?

Focus is shifting from prevention to incident identification and breach reporting, including the timeliness and effectiveness of firms' procedures to respond to cyber-risk events. In addition, organisations are expected to strengthen their risk and control frameworks in terms of quantification of cyber risk, and develop approaches and metrics to measure, report and then improve.

The Discussion Paper marks the beginning of a clear direction of intent for resilience by the regulatory authorities: as such, cyber and resilience emerge as hot topics, encompassing other high-impact and attention domains and initiatives, such as technology resilience, crisis management, incident response and recovery. The operational resilience policy statement is expected in late 2019 or early 2020 to formalise regulatory expectations of resilience.

Find out more

- https://www2.deloitte.com/uk/en/pages/risk/articles/cyber-risk-and-regulation-in-europe.html
- https://www2.deloitte.com/uk/en/pages/risk/articles/operational-resilience-in-financial-services.html

Deloitte contacts

Mike Sobers
Partner
msobers@Deloitte.co.uk

Yannis Petras
Director
ypetras@deloitte.co.uk

6.2 Disruptive Technologies and Digitalisation

Why is it important?

Disruptive technologies and the era of digitalisation is here to stay. Technological advances and trends in advanced analytics, robotic process automation (RPA), blockchain and cognitive intelligence, including Artificial Intelligence, are rapidly transforming organisations. They reshape business models and enable innovation in terms of productivity and operational efficiency but also, critically, in the way they connect with, and offer products and services to, their customers.

What's new?

These technologies are rapidly advancing, with more interconnected and powerful networks, high-performance computing, and the advent of digital tools, including data analytics, RPA, and machine learning-based tools.

Although the regulation in this area is catching up, there have been some recent developments. The EU Commission published the steps it is taking for "building trust in Artificial Intelligence (AI)", which includes the publication of the final Ethics Guidelines for Trustworthy AI, aiming to encourage public and private investment in AI and related technologies, whilst managing the risks.

What should Internal Audit be doing?

Area of focus	Description
Methodology and Internal Audit framework	Internal Audit should establish a framework and methodology for auditing such technologies: this should be based on a multi-disciplinary approach to risk, and not rely purely on technology risk domains. AI is less about completely new risks, but about a multitude of existing ones that may be harder to identify, given the complexity and speed of solutions. Risks may manifest in unfamiliar ways and with unprecedented velocity and impact.
Consider 'ethical' requirements for the development of AI	Internal Audit should assess whether the ethical requirements are appropriately implemented. Where the Ethics Guidelines indicate that to be "trustworthy", an AI application should: (i) comply with the law; (ii) fulfil ethical principles; and (iii) be robust. They highlight a list of seven key requirements that AI applications should respect to be considered trustworthy: (i) human agency and oversight; (ii) technical robustness and safety; (iii) privacy and data governance; (iv) transparency; (v) diversity, non-discrimination and fairness; (vi) societal and environmental well-being; and (vii) accountability. The document by the EU Commission also presents an assessment list to help check whether these requirements are fulfilled.
Regulatory developments	Functions should stay close to the global regulatory developments, as this may influence the approach to adopt. In anticipation of clear supervisory guidance, the CIIA Global Perspectives paper on AI offers some insights, but we also recommend that Audit leverage the principles of existing supervisory statements relating to use of algorithmic trading, supervision of models, operational, cyber and technology resilience, the Senior Managers and Certification Regime and general requirements on IT controls.

6.2 Disruptive Technologies and Digitalisation

Are there any potential challenges?

Challenge	Description
Maturity and IA focus	The rate of adoption of disruptive technologies may be different for each company, consequently the approach and maturity levels of each Internal Audit department to respond to the risks posed will vary. This depends on the organisation's maturity level and the strategic goals of the Internal Audit department. The challenge remains however: auditors need to accept that the business will be 'disrupted' and need to stay ahead in delivering high quality assurance and independent value-adding advice.
Impact and risk assessment	While some may be more mature with their approach than others, most departments are in the early phases of the journey. In all cases, assessing the impact of such technologies on the existing control environment is imperative to their successful adoption. These risks can be addressed by extending existing approaches to managing enterprise risk, as such Internal Audit needs to assess whether appropriate controls are being implemented to prevent and detect new and emerging risks. Internal Audit should find a balance among the following responsibilities as a value-add function: Assure, Advise, Anticipate.
Traceability and auditability	AI solutions are developed to 'learn' and evolve their capabilities over time, making it inherently challenging to completely decode their decision-processing layers, which in turn makes auditability and traceability of the decision-making rationale challenging.

What Internal Audit skills are required?

In terms of talent and skills, functions should be looking for the optimal blend of all-rounder IT auditors that can easily understand risks' exposures by a new IT solution and assumptions made by them, and specialists or data scientists that can delve deep into risks of AI and new algorithms (for example).

What's next?

The EU Commission's announcements highlight that the ethical dimension when it comes to disrupting new technologies is increasingly becoming a priority and will need to become an integral part of firms' developments in this area. It is important for Internal Audit to start challenging the seven key requirements for trustworthy AI to be integrated in both the solutions their firms are deploying, as well as those that are already in use.

Find out more

- https://www2.deloitte.com/uk/en/pages/financial-services/articles/ai-and-risk-management.html
- https://www2.deloitte.com/uk/en/pages/risk/solutions/technology-and-digital-risk-management.html

Deloitte contacts

Mike Sobers
Partner
msobers@Deloitte.co.uk

Yannis Petras
Director
ypetras@deloitte.co.uk

6.3 Blockchain

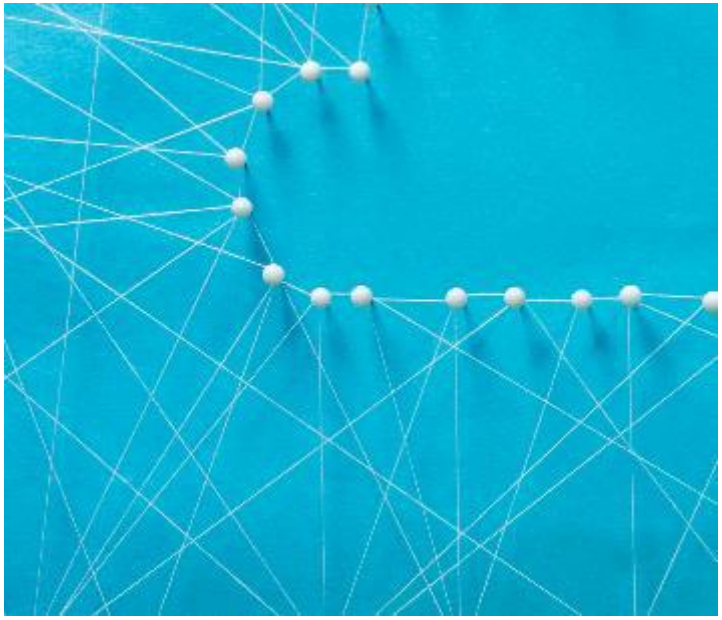
Why is it important?

According to a 2018 report by Gartner, the business value from blockchain will reach $3.1 trillion by 2030 through cost reduction and revenue growth. According to its CEO Survey, 25 percent of participating CEOs perceive the impact of blockchain to be either "major" or "transformational".

What's new?

What exactly do we mean by blockchain? It is effectively a digital, secure, decentralised, distributed ledger which secures (via encryption) and tracks digital transactions. Blockchain was invented as the public transaction ledger of the cryptocurrency bitcoin, a currency without the need of a trusted authority or central server.

Benefits include automation, transaction simplification, enhanced transparency in core business functions (supply chain management, back-office operations and compliance for instance) and help in the reduction of fraud.



What should Internal Audit be doing?

Area of focus	Description
Technology and operational risks	Internal Audit should assess technology and operational risks related to Blockchain. These risks are similar to those associated with current business processes but with additional nuances and different impact or velocity when they materialise. For example, due to inappropriate design architecture decisions, blockchain solutions may not be sufficiently distributed or scalable to meet long term business requirements. In addition, the loss, damage or access of a malicious actor to a user's private key may result in irreversible loss of access to crypto assets.
Value transfer risks	Internal Audit should assess whether Blockchain value transfer risks are appropriately addressed in the Audit. Blockchain enables peer-to-peer transfer of value (assets, identity, or information) without the need for a central intermediary, thereby exposing the interacting parties to new risks that may have been previously managed by central intermediaries.
Smart contract risks	Internal Audit should assess the risks associated with encoding complex business, financial, and legal arrangements on the Blockchain. For example, due to the infancy of the technology, smart contracts may not be recognised as legally enforceable by courts of law due to lack of appropriate precedent.

6.3 Blockchain

Are there any potential challenges?

Challenge	Description
The ongoing role of Internal Audit	While not a pressing need for the majority of Internal Audit functions to react immediately to this emerging risk, as it will largely depend on the rate of adoption of the technology in each institution, it is a commonly shared belief that blockchain is the next step in the digital evolution. Such developments will require Internal Audit to remain a value-adding and impactful function by understanding the specific implementations of blockchain technology, upskill the team to truly understand the emerging and existing risks that the technology is susceptible to, and stay ahead of the curve. Internal Audit's role in anticipating/evaluating newer risks to the organisation is once again key, as many businesses are running innovation labs and continue to evaluate the use of the technology. Moreover, given that blockchain is still being seen as a black box and intrinsically complex, associated with a high risk technological development, internal audit should be able to separate facts from fiction, and provide a clear, objective and timely view.

What Internal Audit skills are required?

Functions should be looking for the optimal blend of all-rounder IT auditors who:

- understand risk exposure from new IT solutions; and
- understand the business processes.

What's next?

The bitcoin design and the use of the blockchain principles, has inspired other applications and enterprise uses. Deloitte global survey of more than 1,000 global blockchain-savvy executives from seven countries indicates that momentum is shifting from a focus on learning and exploring the potential of the technology to identifying and building practical business applications.

For example, 74 percent of those surveyed, report that their organizations see a "compelling business case" for the use of blockchain and many of these organizations are moving forward with the technology. About half of that number (34 percent) report that their organization already has some blockchain system in production while another 41 percent of respondents say they expect their organizations to deploy blockchain applications within the next 12 months.

Find out more

- https://www2.deloitte.com/insights/us/en/topics/understanding-blockchain-potential/global-blockchain-survey.html

Deloitte contacts

Mike Sobers
Partner
msobers@Deloitte.co.uk

Yannis Petras
Director
ypetras@deloitte.co.uk

6.4 Cloud Governance and Security

Why is it important?

Cloud adoption has seen a significant upward trajectory over the past few years, with the worldwide public cloud services market for Cloud Service Providers growing by c 21% to $186 billion total revenues in 2018. It is projected to grow another 63% over the next three years. There is no denying that cloud in financial services is here to stay, and emerging as one of the 'hot' topics for IT Internal Audit functions in 2020.

What's new?

The transformational benefits of Cloud technologies, such as flexibility (pay-as-you-go), technological sophistication, cost and tax efficiency, customer empowerment, are undeniable, and have fueled the exponential rise in its popularity and successful adoption.

The risks, however, if not managed carefully can be significant. There have been some significant issues and failures that have hit the news recently. A glitch at a major cloud service provider (CSP) in 2017 caused hundreds of thousands of websites using its services to function badly or not at all for a few hours.

Lloyds, the specialist insurer, estimated in a report published in January 2018 that if an extreme cyber incident took a top cloud provider offline for three to six days it would cost US businesses around $15 billion. Lloyds is flagging the risk of even worse to come.

What should Internal Audit be doing?

Area of focus	Description
Cloud governance and strategy	Internal Audit should assess the benefits realisation; business alignment; appropriateness of cloud service model and deployment type (given the type of service, data and risk appetite of the organisation); selection of the right CSP and appropriate ongoing oversight. Additionally Internal Audit should include a review of the shared responsibility and accountability model, as migrating IT-services towards the cloud doesn't yield a shift in accountability. Although responsibilities can be transferred (e.g. infrastructure and platform security with usage of a SaaS-application), the cloud consumer always remains accountable for the governing and safeguarding of its data.
Technology integration	While designing the audit plan Internal Audit should consider the complexity of integration with legacy platforms; deployment impact across the technology estate; project assurance over transformational or integration initiatives and security controls relevant to cloud governance and security.
Compliance, legal and risk management	Internal Audit should assess the data privacy considerations including physical location of data; broader operational and compliance risks; implications of GDPR and complying with other national laws.

6.4 Cloud Governance and Security

Are there any potential challenges?

Challenge	Description
Maturity and IA focus	Despite the expansion and level of maturity, in adoption, benefits and technology, using the cloud is not straightforward. Even though a large part of the IT function is handed over to a cloud service provider – and with it, much of the operational hassle – users still bear the ultimate risks and responsibilities if things go wrong.
Impact and risk assessment	Further to the above, it is imperative that risk, assurance and control functions ensure that businesses remain on top of the risks. While security at Cloud Service Providers level has noticeably matured and improved in recent years, the greater risk to security remains within the user organisations' control, for example in the way they manage access rights, or the level of discipline applied to monitoring and changes in configuration. It is also key to recognise that the cloud consumer always remains accountable for the governing and safeguarding of its data (including data discovery, classification, assessing and mitigating risks of data exposure) while the cloud provider is responsible to address operational, security and privacy concerns.

What Internal Audit skills are required?

A combination of change assurance (in the case of cloud transformation programmes), infrastructure technology, third party/supplier management and cyber security skill will be key to appropriately mitigate the risks around cloud technologies.

Find out more

- https://www2.deloitte.com/uk/en/pages/consulting/topics/cloud.html
- https://www2.deloitte.com/uk/en/pages/consulting/solutions/managing-risk-and-cyber-security-with-cloud.html

Deloitte contacts

Mike Sobers
Partner
msobers@Deloitte.co.uk

Yannis Petras
Director
ypetras@deloitte.co.uk

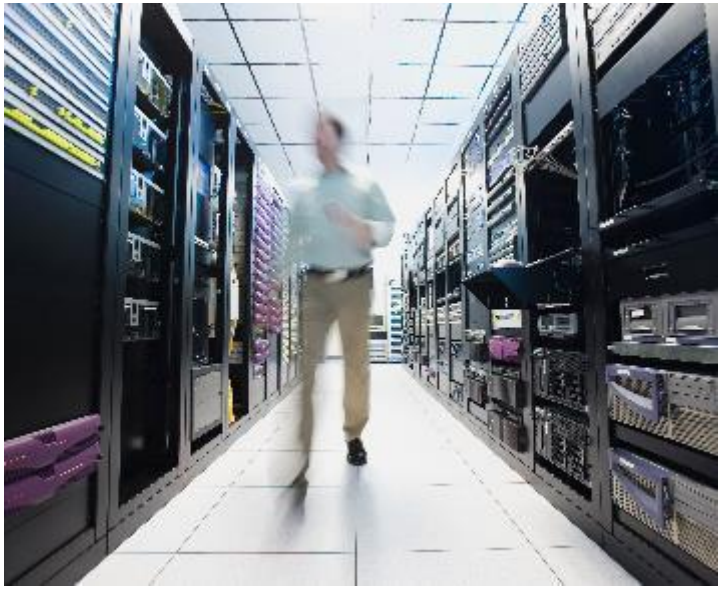
6.5 Data Privacy and GDPR

Why is it important?

The General Data Protection Regulation (GDPR) came into force in May 2018. The regulation carries significant regulatory fines for breaches, up to 4% global annual turnover. This coupled with reputational damage, means Data Protection is now a major ongoing risk to firms. In some sectors such as banking and insurance, there are multiple regulators focused in this area including the Information Commissioners Office (ICO) and the FCA. Many millions of fines are currently issued by ICO to firms. Internal Audit have a critical role to play in assessing the ability of firms to prevent and detect GDPR breaches which may give rise to regulatory penalty and public censure, both of which have significant reputational impacts.

What's new?

- The GDPR came into force in May 2018.
- The policies, procedures and controls implemented to meet GDPR; should have been in place for the last 12- 15 months. Firms are now expected to continually focus on the adequacy of their frameworks and the embedding of these frameworks in the business.
- Regulators expect organisations to have a demonstrable compliance of GDPR, thus Internal Audit plays a key part of the GDPR compliance framework.



What should Internal Audit be doing?

Area of focus	Description
Auditing the completed GDPR programme	Audit the GDPR compliance framework, with the key focus on implemented governance structures, roles and responsibilities; assessment of the key areas of the regulation: - Third party data processors; - Records of data processing activities; - Lawful basis for data processing; - Fair data collection and processing; - Data privacy by design and by default; and - International transfers.
Deeper focus on high risk functions	Hold discussions with the Data Protection Officer, Privacy Office and business to understand the areas of focus to ensure audit scoping is pinpointed to areas of greatest risk, for example focus on incident management, marketing and any other functions handling large amounts of personal data.
Deeper focus on areas that handle special category data	Understand and incorporate the regulators' focus and emerging guidance in the audit plan and risk assessment, focusing on special category information including health, criminal records, credit and personal financial data.
Accountability framework and data processing taking place abroad.	Extend the audit to EU data being processed elsewhere. The extra-territorial scope of GDPR applies to personal information of EU citizens held anywhere in the world.

6.5 Data Privacy and GDPR

Are there any potential challenges IA should be aware of?

Challenge	Description
Requirement for SME input	There is often a lack of GDPR expertise within Internal Audit as many requirements of GDPR are new/ revised. Therefore external subject matter experts are typically required to support with planning and execution of the audit where required. Internal Audit should seek knowledge transfer and training from subject matter experts to build knowledge in-house.
Reliance on IA	Instances have been identified where the Business and Data Protection Officer is relying on Internal Audit to identify gaps rather than via first or second line oversight.
Scope of audit	Given the broad applicability of GDPR a risk-based approach is required to determine the phasing of Internal Audit's work, ensuring all high risk functions are covered within a reasonable period.
Brexit	Internal Audit should make enquiries to ensure Brexit implications are being considered by firms to ensure compliance with GDPR.

What Internal Audit skills are required?

- Subject matter knowledge of GDPR.
- Ability to communicate the risks to very senior individuals both in the EU and elsewhere, and manage multiple stakeholder interest in any given finding.
- Knowledge of Regulators such as the ICO and FCA as well as EU regulators and their priorities.
- Ability to rate the risks based on market insight, regulatory actions and interests.

What's next?

- In the next few years there will be huge demand for Internal Audit and compliance assessments and increased demand for SME support as Internal Audit teams develop their skills to audit GDPR.
- Internal Audit may be requested to perform ad-hoc assessments as organisations fear emerging large fines.
- Audit of Third Party suppliers will also see an increase as these are mandatory under the GDPR.

Find out more

- https://www2.deloitte.com/uk/en/pages/impact-report-2018/articles/brexit-navigating-change.html
- https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

Deloitte contacts

Balavernie Sritharan
Director
bsritharan@deloitte.co.uk

Contacts – Financial Services Internal Audit

Russell Davis

Partner, Banking and Capital Markets

020 7007 6755

rdavis@deloitte.co.uk

Matthew Cox

Partner, Insurance

020 7303 2239

macox@deloitte.co.uk

Aaron Oxborough

Partner, Insurance

020 7007 7756

aoxborough@deloitte.co.uk

Terri Fielding

Partner, Investment Management and Private Equity

020 7303 8403

tfielding@deloitte.co.uk

Mike Sobers

Partner, Technology

020 7007 0483

msobers@deloitte.co.uk

Matt Cheetham

Partner, Regions (South)

0117 9841 158

mcheetham@deloitte.co.uk

Jamie Young

Partner, Regions (North)

0113 292 1256

jayoung@deloitte.co.uk

Stephen Williams

Partner, Regions (Scotland)

0131 535 7463

stephenwilliams@deloitte.co.uk

Deloitte.