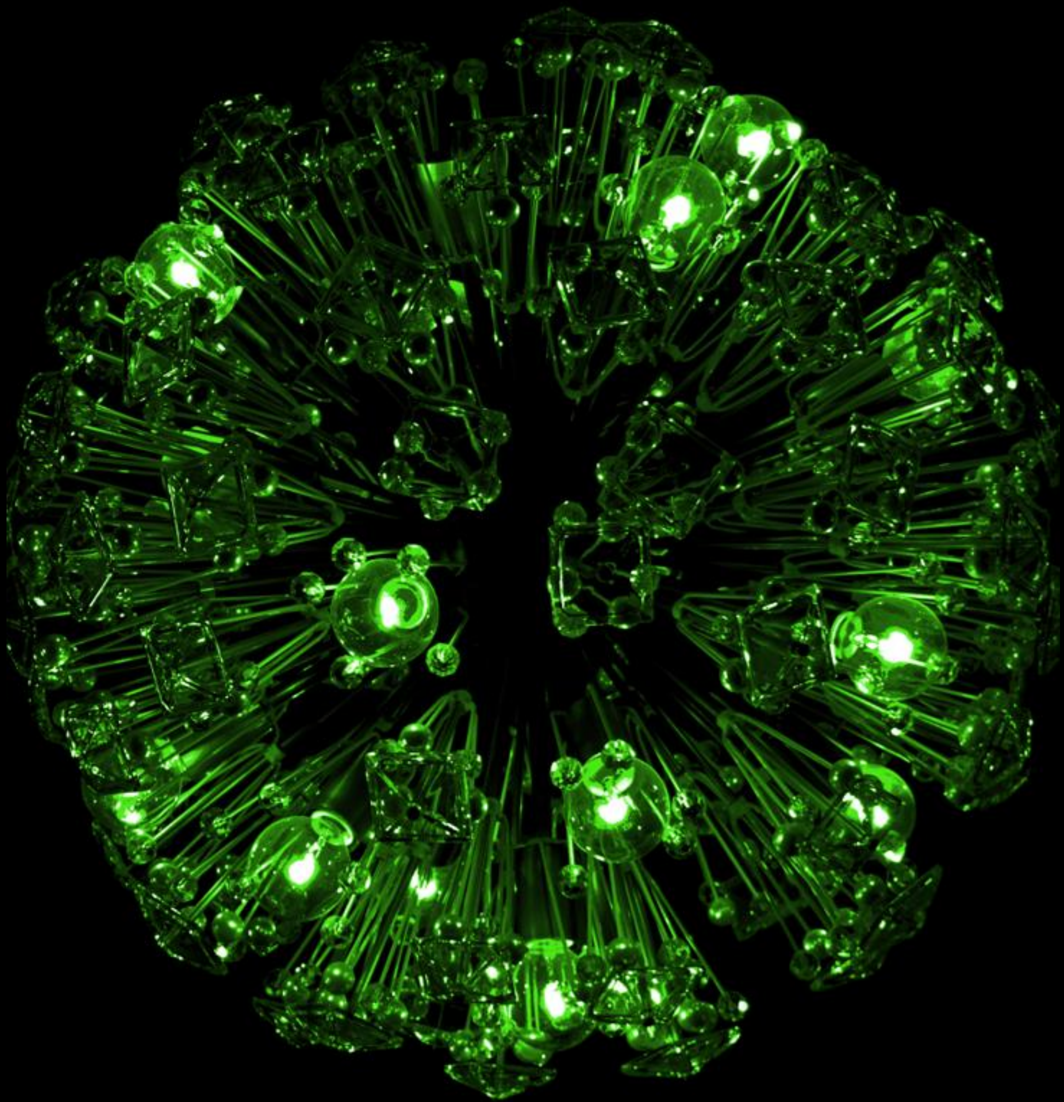


Financial Services Internal Audit

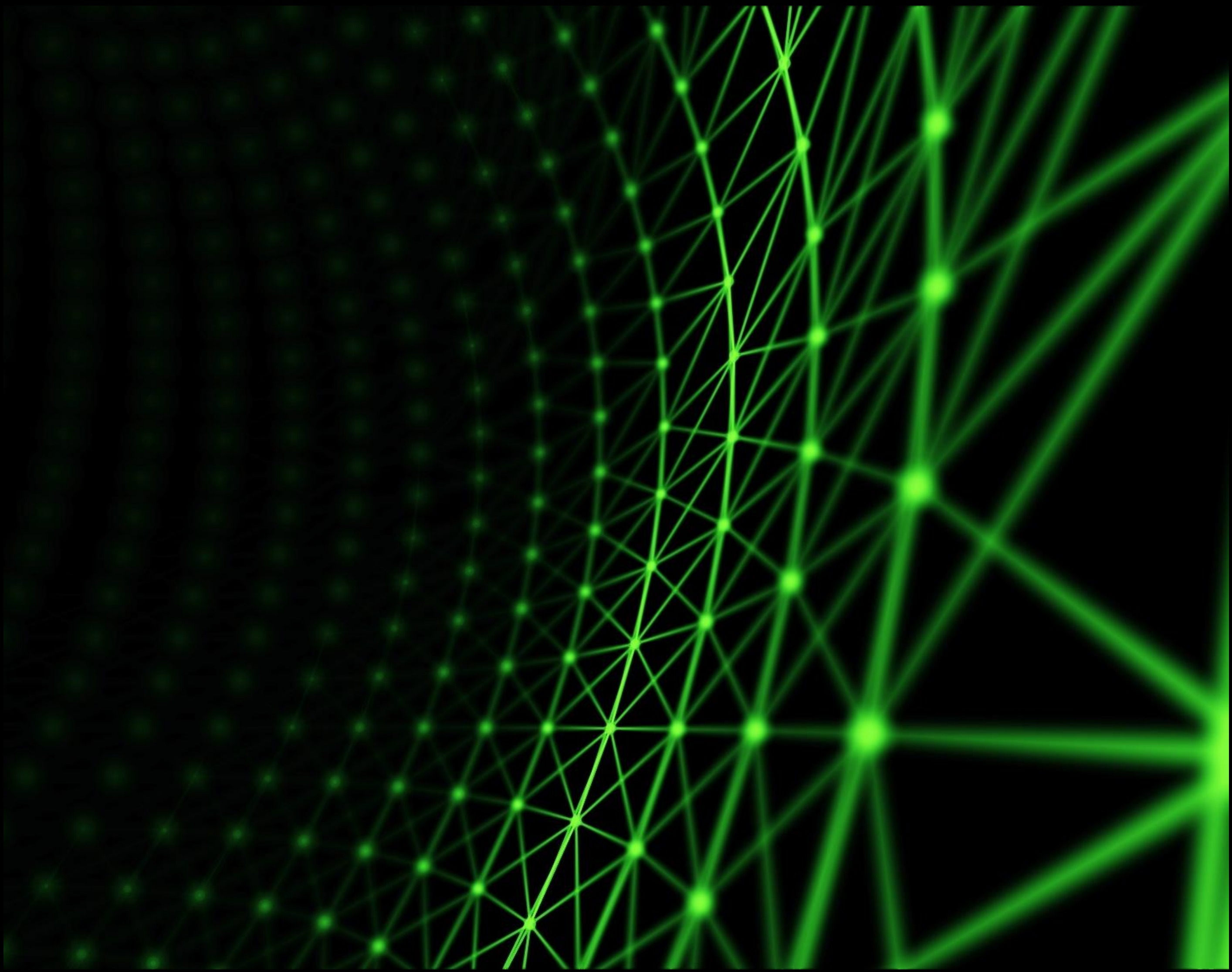
Planning Priorities 2020

Overview

In this publication we provide a snapshot view of our assessment of the Planning Priorities for Internal Audit in Financial Services in 2020. As in previous years we have focused on new areas relevant to Internal Audit, recognising that regulatory, technological and social landscapes continue to evolve as does the role of internal audit in providing assurance and insight.

In 2020, we anticipate an increased emphasis on digital risks, early assurance on areas of upcoming regulatory change (e.g. IBOR reform) as well as a continued focus on conduct, culture and governance. IA teams need to be prepared to respond to a continually changing environment – developing the auditors and Internal Audit functions of the future.

We hope this summary helps inform your 2020 planning and we encourage you to read our chapters to find out more.



Our view of the Internal Audit (IA) suggested areas of focus within this publication

Consistent focus of IA compared to 2018/19

Increased focus of IA compared to 2018/19

Significant increased focus of IA compared to 2018/2019

Contents

Industry icons

- Banking and Capital Markets
- Insurance
- Investment and Private Equity

1. Regulatory

Ten years after the financial crisis most post-crisis prudential policies have now been decided, and banks in particular are now much better capitalised and more liquid than before the crisis. Nonetheless, regulatory scrutiny remains heightened across financial services. Firms need to be prepared to respond to the ever-changing focus of the regulator.

Our view of the change in IA focus from prior year to now:

Regulatory hot topics for 2020		IA suggested areas of focus
1.1	IBOR Reform	Significant increased focus of IA compared to 2018/19
1.2	Consumer Finance – motor finance and beyond	Significant increased focus of IA compared to 2018/19
1.3	Algorithmic Trading	Significant increased focus of IA compared to 2018/19
1.4	Tax Compliance – FATCA/CRS	Consistent focus of IA compared to 2018/19
1.5	Tax Strategies and Responsible tax	Increased focus of IA compared to 2018/19
1.6	Operational Resilience	Significant increased focus of IA compared to 2018/19
1.7	Financial Crime	Consistent focus of IA compared to 2018/19

1.1 IBOR Reform

Overview

The clock is ticking for firms using key interbank-offered rates (IBORs), such as LIBOR, and market participants exposed to them, due to the transition away from IBORs to Alternative Reference Rates (ARRs) such as Sterling Overnight Index Average (SONIA). The FCA will not compel the banks who contribute to LIBOR to continue to do so beyond 2021, meaning the viability of LIBOR continuing cannot be guaranteed beyond that date; other benchmarks such as Euro Overnight Index Average (EONIA) will also be reforming to €STR ('Euro Short-Term Rate') by 2022.

In June 2019, the FCA and PRA provided feedback to the market in their 'Dear CEO Letter' sent to large banks and insurers on LIBOR reforms. The focus of the feedback is on the identification and quantification of LIBOR usage and exposures and the management of risks associated with it. Whilst there has been tangible progress across the industry, a number of firms are yet to formalise their plans for the transition.

Working groups from each of the Central Banks for the UK, US, Eurozone, Switzerland and Japan have been tasked with driving consensus and establishing market standards to ease the transition.

IA's role

Given IBOR's extensive use in the financial markets and the significant exposures for market participants, IA should consider reviewing:

- Progress of IBOR programmes and expected timing of complete transition.
- Adequacy of work conducted to evaluate the financial impact across all product lines as a result of the switch from IBORs to ARRs.
- Adequacy of stakeholder involvement, governance and approval of valuation methodologies and resulting implications (e.g. impact on hedging strategies).

1.2 Consumer Finance – motor finance and beyond

Overview

There is greater regulatory focus on mainstream forms of finance and insurance. A recent FCA thematic review concluded that issues exist within both lenders and brokers arising from consumer borrowing to finance motor vehicles.

The regulator's direction of travel is to investigate areas of potential consumer harm such as unfair treatment in rent-to-own, high cost short-term credit and insurance distribution channels which may represent established sources of income for many firms.

Unfair treatment or potential consumer harm, can manifest in a number of different ways:

- Poorly designed products which do not consider the needs and circumstances of consumers.
- Non-identification of potentially vulnerable consumers.
- Unsuitable or unfit distribution channels which increase the risk of mis-selling.

IA's role

IA should consider a review of sources of income within firms to identify areas where there could be considered to be unfair treatment of consumers, considering the risk and reward associated with these income streams.

Specific consideration should be given to:

- Affordability assessments and lending decisions.
- Review of commission element of premium income to ensure that customer value is not eroded by lengthy distribution chains.

1.3 Algorithmic Trading

Overview

The finance sector is becoming increasingly automated, with many firms using or interacting with algorithms. The number of trading algorithms in active use has significantly increased in recent years. This trend is driving operational efficiencies, lowering costs and enabling firms to gain a competitive advantage.

There are specific requirements covering algorithms to ensure accountability and fairness in the use of algorithms. The specific requirements are set out in Markets in Financial Instruments Directives II Regulatory Technical Standard 6 (MiFID II RTS 6), in conjunction with various publications by the FCA, PRA and FICC Markets Standards Board (FMSB); these require detailed consideration by firms.

IA's role

Assurance by IA should include a gap analysis of compliance with regulatory requirements and guidance, but should also consider:

- The adequacy of the algorithmic trading control framework.
- The adequacy of the approach algorithm validation.
- Effectiveness of the governance structure for oversight of algorithms.
- Effectiveness of testing and deployment of algorithmic trading.
- Adequacy of the annual self-assessment process.
- Controls over approach to real-time monitoring of algorithms.

1.4 Tax Compliance – FATCA and CRS

Overview	With both the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) regimes now fully implemented and reporting in their third/fourth year, there has been a shift in focus by tax authorities from implementation to enforcement. In the UK, HMRC have opened the first enquiries into returns, while French tax authorities have opened compliance audits. Meanwhile, the Organisation for Economic Co-operation and Development (OECD) has requested that tax authorities report soon on enforcement efforts. This will likely lead to more formal requirements being set.
IA's role	IA should consider a review of controls and governance over these regimes in order to be able to respond to any upcoming tax authority requests. IA should also consider a full review of a firm's tax programme as compliance is largely untested in the majority of firms.

1.5 Tax Strategies and Responsible Tax

Overview	Public and media scrutiny of firms' tax affairs remains widespread. Tax authorities in many countries feel increasingly empowered to robustly challenge any perceived tax avoidance arrangements and tax is now firmly on the boardroom agenda. In addition, a number of regulatory tax developments are taking effect during 2019/ 2020, including HMRC's new business risk review approach (October 2019) and Making Tax Digital for VAT ("MTDfV") (this took effect for many businesses from April 2019, although there are deferrals to later in 2019 for more complex firms). The challenge for firms is to ensure compliance with the tax requirements.
IA's role	IA has an increasingly important role to play in supporting the tax function to ensure it responds effectively to the regulatory change, in particular by carrying out periodic, targeted testing of the operation of controls over key tax risks. Taxpayers are expected to not only have adequate policies and processes in place to ensure correct tax compliance, but also regularly to test those policies and processes. In addition to a focus on tax positions taken by firms and regulatory expectations, IA focus should also include controls and processes over tax advice given to customers to ensure associated compliance, financial and reputational risks are managed.

1.6 Operational Resilience

Overview

Operational resilience is expected to be an increasingly important area of focus for the PRA and FCA over the next few years with regulators seeking to reduce the frequency and impact of operational failures that impact customers, markets and financial stability. This means making critical business services more resilient to the challenges that they face, including keeping pace with the rate of technological change and cyber threats. The PRA and FCA have released a discussion paper (DP1/18) outlining the approach they expect firms to take to improve their operational resilience and implement frameworks to support it. They expect to release a consultation paper later this year.

UK regulators are intervening in a small number of cases, and despite regulatory change still being in the discussion phase, have already requested that 40 small-to-medium sized firms perform an audit of Management Information (MI) covering operational resilience reported to the Board.

IA's role

IA's scope should include:

- Review of governance arrangements supporting the firm's operational resilience work.
- Review of the approach the business has taken to identify critical business services.
- Review of impact tolerances in relation to critical business services.
- Mapping of operational dependencies (e.g. people, system, suppliers and facilities) that support business services in order to identify concentration risks and single points of failure.
- Assessment against the PRA's expectations of communication plans.

1.7 Financial Crime

Overview

The FCA's view, as set out in their 2019-2020 Business Plan, is that the fight against financial crime requires a combined effort of sharing intelligence, data and technology. The Joint Money Laundering Steering Group ("JMLSG") in the UK has set a good example of intra-agency cooperation and industry-led implementation of regulatory compliance. In the coming year, it is anticipated that the FCA will also continue to strengthen their partnership with the National Crime Agency and the Joint Money Laundering Intelligence Taskforce's expert working group to identify and mitigate financial crime risk.

IA's role

IA focus areas should include:

- Assessment of the adequacy of actions and communications to reinforce the fundamental principles of management's behaviour.
- Conducting thematic reviews across the financial crime domain.
- Review of governance framework over enterprise-wide risk assessment activities.
- Assess whether the data analytics solutions adopted by firms are adequately designed, fit for purpose and effectively operated to address financial crime risks.

2. Credit

Credit risk remains core to much of the financial services industry and firms' risk management processes in this area remain an area of regulatory focus. Continued political and economic uncertainty in the UK means that stress testing also remains a key area for businesses.

Our view of the change in IA focus from prior year to now:

Credit hot topics for 2020		IA suggested areas of focus
2.1	Credit Risk Transformation	Increased focus of IA compared to 2018/19
2.2	Stress Testing	Consistent focus of IA compared to 2018/19
2.3	Model Risk Management	Significant increased focus of IA compared to 2018/19

2.1 Credit Risk Transformation

Overview

Regulatory challenges are forcing firms to re-examine the cost, efficiency, sustainability and transparency in the quantification techniques and systems used in the credit decisioning process. With the help of technology, firms are improving their end-to-end credit risk management process in order to address these challenges, for example:

- Some retail banks are commencing digital change programmes aimed at transforming the customer experience across the on-boarding journey.
- Commercial and corporate banking firms are focusing on making credit risk management processes more customer centric and efficient, implementing new fin-tech or cloud-based solutions, embedding processes, technologies and ways of working that will underpin the enablement of a more agile organisation.

IA's role

IA has an important role to play in providing assurance over new or changed credit risk management systems, with a focus on ensuring solutions are aligned to the firm's strategic objectives, the scale and nature of its business and its risk profile. Examples of IA focus areas include:

- Credit risk management functionality.
- Risks associated with the use of alternative data sources such as Open Banking and small and medium-sized entity credit data sharing schemes.
- Third party risk management and data protection and privacy requirements associated with the use of financial technology and the use of Artificial Intelligence in decision-making and decision support models.
- Undertaking dynamic control testing processes over the components of the credit risk management framework (including risk appetites, automated lending processing including underwriting, early warning and watch list processes and collections and recoveries/ re-structuring).

2.2 Stress Testing

Overview	In 2020, greater attention is expected to be given by firms to the adequacy of stress testing programmes. Regulatory developments are also expected to require focus over the year ahead as, for example the Bank of England, the Federal Reserve and the European Banking Authority (EBA) are all expected to reassess their respective approaches to concurrent stress testing for 2020 onwards.
IA's role	IA's role should be focused on the following key areas: • Review the level of coordination and cohesion in the firm's stress testing approach. • Review the readiness of stress testing approach including IFRS 9 and Climate Change being new topics to be addressed in the stress testing approach. • Adequacy of timing of generation of stress testing results. • Level of evidence of continuous process and methodological improvement. • Adequacy of governance framework, risk management controls and documentation around processes and assumptions, in particular expert judgement and post-model adjustments.

2.3 Model Risk Management

Overview	Regulatory expectations for model risk management continue to evolve for all firms using models in their business, with the scope, breadth and depth of model development, use and oversight activities all increasing. Supervisors will neither approve nor place reliance on the firm's strategic and operational use of a model, including for risk assessment, capital planning and stress testing, unless satisfied with a firm's model risk management.
IA's role	Regulators have specific expectations relating to IA's role in Model Risk. IA is expected to carry out an overarching risk assessment of all aspects of model risk, drawing up multiyear IA programmes with targeted work plans structured to challenge the model governance framework and test the effectiveness of model risk controls. Particular areas of focus for IA should include: • Adequacy of the board's oversight and challenge of models. • Independent model validation. • Adequacy of organisational maturity of model risk management. • Risks associated with the use of alternative data sources, third party risk management, data protection and privacy requirements associated with the use of financial technology in ecosystem type environments and the use of Artificial Intelligence in decisioning and decision support models.

3. Financial

IFRS 9, 15 and 16 have been implemented by firms, although these new standards continue to be embedded, and regulators continue to seeking greater harmony in firms' IFRS 9 approaches. The focus of regulators and firms has now expanded to IFRS 17, which represents a fundamental change to the way insurers report to the market. Additionally, the financial sector has a key role to play in the transition to a lower-carbon economy. A new type of risk will affect firms and their Internal Audit plans going forward.

Our view of the change in IA focus from prior year to now:

Financial hot topics for 2020		IA suggested areas of focus
3.1	IFRS 17 IFRS 9	Increased focus of IA compared to 2018/19
		Consistent focus of IA compared to 2018/19
3.2	Climate Change	Significant increased focus of IA compared to 2018/19

3.1 IFRS 17 and 9

Overview	IFRS 17 (Insurance Contracts) has been described as the most significant change to insurance accounting for a generation, similar in scale and complexity to the implementation of Solvency II in 2016. The Standard will bring the industry closer to a 'margin' model of accounting, showing insurance revenues and insurance service expenses separately. This will enable the market to better compare insurers across industries. This reporting change will have a knock-on effect on all parts of a business and introduce a need for new data, systems and ways of working. The UK banking industry, in particular the large UK retail banks, has invested significant resources to update financial and regulatory reporting for IFRS 9 (Financial Instruments). The shift now moves to embedding the new Standard, and implementing strategic solutions within IFRS 9 modelling to replace tactical ones. Firms are also reflecting on regulatory feedback on their approaches in particular in response to the PRA's Dear CFO letter issued in April 2019, and in some cases considering changes to their IFRS 9 methodologies.
IA's role	On IFRS 17, IA should consider performing reviews over business readiness for new standards from a project governance, technology and resourcing perspective, including second-order impacts such as investor relations and reward. IA should also consider providing early assurance over technology solutions implemented to improve firms' reporting capabilities. On IFRS 9, IA should focus on governance over model and methodology refinements and ongoing operational effectiveness of controls. IA should also consider the following areas in scope, which reflect areas of complexity and/or regulatory focus: • Sensitivity disclosures. • Assumptions about customer behaviour ('behavioural lives'). • Significant increases in credit risk. • Post-model adjustments. • Multiple economic scenarios.

3.2 Climate Change

Overview	Climate change and the resulting catastrophic effects on the environment have never been more apparent. Government bodies have begun to take action through legal frameworks and global initiatives such as The Paris Agreement. There is now increased pressure on the financial sector to recognise its critical role in transitioning to a lower-carbon economy and the recent UK net zero legislation are just some of the major adaptations to legal frameworks, which highlight the need to take action. The FCA and PRA recognise that the risks arising from climate change, be they transitional or physical, will have an impact on firm's strategic objectives. Additionally, firms need to disclose in the financial statements the financial impact of climate change, recognising that failure to do so may impact investor decisions. It is essential that firms recognise the need to engage with regulatory bodies to advance the development of their approach to managing climate change-related risks.
IA's role	IA focus areas should include: • Review of risk management and governance frameworks to determine if the design facilitates effective discussion and management of climate change related risks. • Assess the level of collaboration within firms, ensuring firm-wide understanding of the potential impact that climate change poses. • Assess the understanding of the varying levels of climate related physical and transition risks to which the firm is exposed and how these manifest within each business line. • Review of progress relative to regulatory statements and guidance (e.g. the PRA's supervisory statement 3/19).

4. Governance, Risk Management and Culture

Regulatory pressure continues to drive major change in firms' governance, risk management and culture, particularly through the introduction of the Senior Manager and Certification Regime (SMCR) in the UK. There is an increased focus on the roles and responsibilities of the second line of defence, business culture, psychological safety at the workplace and the use of remuneration structures to encourage ethical behaviour towards customers.

Our view of the change in IA focus from prior year to now:

Governance, risk management and culture hot topics for 2020		IA suggested areas of focus
4.1	Governance Culture in Financial Services	Significant increased focus of IA compared to 2018/19
4.2	Second Line of Defence	Increased focus of IA compared to 2018/19
4.3	Risk Appetite and Risk Culture	Increased focus of IA compared to 2018/19
4.4	Psychological Safety	Significant increased focus of IA compared to 2018/19
4.5	Remuneration – Risk and Reward	Significant increased focus of IA compared to 2018/19

4.1 Governance Culture in Financial Services

Overview

Robust corporate governance arrangements are key to driving good culture and desired behaviour within firms. Corporate governance and culture will be at the forefront of the regulatory agenda in 2020, heightened by the implementation of the Senior Managers and Certification Regime ('SMCR') in prior years, which is designed to reinforce the concept of individual accountability for Senior Managers to ensure they demonstrate their adherence to Conduct rules.

There are a number of areas relating to SMCR upon which firms should continue to focus:

- Clearly defining responsibilities and articulating the delineation between individual's responsibilities, specifically in areas that impact all areas of the business such as technology and operations.
- Documenting reasonable steps that are taken in a consistent and practical way.
- Ensuring that Fit and Proper assessments are robust and adequately documented.

IA's role

IA are already focusing on this area and the frequency and robustness of reviews carried out over corporate governance frameworks and board effectiveness is expected to increase. IA's focus areas should include:

- Review of governance arrangements.
- Robustness and review of the risk management framework.
- Alignment of the risk management framework to the achievement of a firm's strategy.
- Monitoring of the effectiveness of changes made.
- Assessment of the adequacy of actions and communications to reinforce the fundamental principles of the norms of behaviour of those charged with governance.

4.2 Second Line of Defence

Overview	The FCA re-iterated in their 2019-20 business plan the importance of effective governance. A governance framework demonstrating appropriate three lines of defence responsibilities supports effective governance. Currently, there remains a high level of regulatory focus on the effectiveness of the second line of defence. Potential challenges, particularly relating to the second line of defence include: reliance by second line on IA to 'plug the gaps' in second line monitoring and second line undertaking first line activities due to a perceived risk of lack of capability or capacity within the first line.
IA's role	IA should consider: • The roles and responsibilities of Second Line Risk and Compliance in the governance structure. • Outputs from Second Line Risk and Compliance in day-to-day decision-making. • Whether there is effective oversight of emerging industry issues/regulatory concerns.

4.3 Risk Appetite and Risk Culture

Overview	The FCA wish to promote healthy cultures within firms, which in turn should have the leadership capability to create and maintain these cultures. One area of focus relates to remuneration structures to ensure that they do not encourage behaviours or practices amongst staff which could result in unfair outcomes for customers, or harm the broader financial market. The regulator expects firms in the next year to demonstrate awareness of culture, take steps to address any issues and reflect in their business practices. There is a need to ensure Non-Executive Directors challenge Executive Directors on adherence to Risk Appetite and that these risk appetites are clearly documented in documents such as Operational Risk Self-Assessments to promote good decision making.
IA's role	IA should consider: • Reviewing adherence to risk appetite documented policies and procedures. • Reviewing controls over the management of conflicts of interest within commercial arrangements, which may drive inappropriate behaviour and controls that ensure customer interests are protected. • Performing a focused review of the culture indicators within the firm, how they are embedded into the strategy and how this is measured and monitored. • Validating the remuneration and incentive arrangements across all parts of the firm to ensure they are effective in encouraging a customer-centric culture.

4.4 Psychological Safety

Overview	The term 'psychological safety' is used to describe a workplace where employees feel safe to express new ideas, raise issues, challenge unethical behaviour and voice concerns without the fear or sense of embarrassment, punishment, retribution or rejection. The FCA focuses on creating a psychologically safe environment within the financial services industry. The FCA conducted its first CultureSprint focused on creating a speak up, listen up culture across the financial services industry. The FCA considers psychological safety particularly important within Financial Services, as it prevents employees from pursuing the best customer outcomes in the face of traditional behaviours and incentive structures and is therefore considered to be a contributing factor in major firm failures.
IA's role	IA has an important role to play including: • Reviewing the tone at the top, including seeking evidence to demonstrate senior management are promoting a culture of psychological safety. • Assessing the design and operating effectiveness of initiatives that promote a psychologically safe environment, particularly with regards to risk and controls. • Reflecting on audit findings and opining on psychological safety through the assessment of stakeholder behaviours observed during audits (including when discussing audit findings) and whether they support psychological safety. IA has typically found explicit discussion of culture to be difficult, however, leveraging the concept of psychological safety when commenting on culture in both IA reports and Audit Committee papers can be helpful.

4.5 Remuneration – Risk and Reward

Overview	In recent years, the regulatory and governance framework in many financial services firms has become increasingly complex. Within the insurance industry, the Insurance Distribution Directive (IDD) is now in effect and is designed to enhance consumer protection when buying insurance and to support competition between insurance distributors. IDD has forced firms to re-evaluate their remuneration structures and to design and implement remuneration policies and procedures in compliance with IDD.
IA's role	Firms should be planning annual reviews of their remuneration policies, processes and implementation in light of the remuneration regulatory requirements. IA's approach should take account of relevant financial services regulation and make use of reward specialists in this rapidly evolving area. Alternatively, IA should assess the rigour and robustness through these annual reviews where they are being performed by another function in the firm (for example, Risk and/or Compliance).

5. Conduct

Conduct risk management remains crucially important within financial services, with focus in the areas of customer journeys and assessment of customer affordability. In particular, the treatment of vulnerable customers should remain high on the agenda for all firms and firms should have in place appropriate processes and controls to identify and monitor the different journeys that customers might face.

In addition, in wholesale markets, there have been recent development in conduct codes and standards which provide a common set of guidelines to promote the integrity and effective functioning of the wholesale markets and also provide a helpful framework which IA can use when defining their audit scopes.

Our view of the change in IA focus from prior year to now:

Conduct hot topics for 2020		IA suggested areas of focus
5.1	Customer Journeys and Culture	Significant increased focus of IA compared to 2018/19
5.2	Retail Conduct – Customer Affordability and Vulnerability	Increased focus of IA compared to 2018/19
5.3	Market Conduct	Significant increased focus of IA compared to 2018/19

5.1 Customer Journeys and Culture

Overview

The FCA expects firms to consider the impact on customers throughout the lifecycle of their products and interactions. Firms are expected to evidence customer centricity by implementing business plans, products and controls that are driven by the desire to provide fair customer outcomes.

The FCA has continued to emphasise its focus on the treatments applied to vulnerable customers. Consideration is now being given to how firms establish and monitor the differing journeys these customers may and should face.

IA's role

IA have unique access across firms that facilitate the independent assessment of customer journeys from start to finish and, by focusing on the assessment of customer journeys through end-to-end outcomes testing, the real customer impact can be understood without the limitations of traditional process and controls testing. Outcomes testing often provides invaluable and unique insights into cultural weaknesses and strengths.

In particular, IA should consider:

- Embedding audits of customer journeys within BAU audit scopes.
- Reviewing first and second line documentation of customer interaction points and points of potential influence.
- Identifying and challenging 'non-standard' customer journeys, specifically those that have variations due to identified customer vulnerability.

5.2 Retail Conduct – Customer Affordability and Vulnerability

Overview	Vulnerability continues to be high on the agenda of the industry and the regulator and whilst progress has been made, there remains room for improvement. Vulnerability is a 'state' not a 'trait' – many people will experience some form of vulnerability at some point in their lives; firms have to be flexible and forward thinking in their approach to identifying these changing vulnerabilities and have operations that are designed to address them. In June 2018 the FCA published 'The financial lives of customers across the UK', which summarised key findings from a survey carried out in 2017. Findings from this and earlier studies such as the Financial lives of UK Adults (Oct 2017) continue to highlight the necessity for Industry-wide focus on the improved identification and management of vulnerability. The FCA has acknowledged that creditworthiness and affordability assessments are not an exact science, and that factors outside of normal control, such as a change in the customer's circumstances or wider economic events, can impact affordability. However, firms are expected to have effective processes in place to eliminate lending that is foreseeably unaffordable, without having been too conservative by declining applications where credit would be affordable.
IA's role	Areas of IA focus should include: • Assessment of new 'digital' channels and customer offerings via remote channels to ensure appropriate consideration of customer designs. • Review of business controls designed to enable a reasonable assessment of customers' ability to repay affordably without this significantly affecting their wider financial situation. • Assessment of the treatment of customers through the arrears process.

5.3 Market Conduct

Overview	Wholesale market conduct codes and standards have been developed to provide a common set of guidelines to promote the integrity and effective functioning of the wholesale markets. These codes and standards are intended to promote a robust, fair, liquid, open and appropriately transparent market in which a diverse range of market participants are able to confidently and effectively transact at competitive prices that reflect available market information and in a manner that conforms to acceptable standards of behaviour. Reputable firms have been fined in recent years due to misconduct that led to serious impact on confidence in the UK financial system. In order to prevent similar misconduct and allegations in the future and to restore confidence in Fixed Income Currencies and Commodities (FICC) markets, the Financial Conduct Authority (FCA), Bank of England (BOE) and HM Treasury launched the Fair and Effective Markets review (2015); the FICC Markets Standards Board (2015); the UK Money Markets Code (2017); the FX Global Code (2017); and the Precious Metals Code (2017). The application of wholesale market codes and standards provides a common set of guidelines and does not impose legal or regulatory obligations on market participants. However, in August 2018, the FCA released a policy statement on wholesale market codes of conduct which covers key themes around Governance, Execution, Confirmation & Settlement, Risk Management & Compliance and Information Sharing and how they apply to the FCA Principle 5 under the Senior Manager and Certification Regime (SMCR), where staff ''must observe proper standards of market conduct''. The SMCR was imposed in order to shift responsibilities of activities onto senior managers and increase the scope to Non-Executive Directors. The SMCR guideline applies to all FCA regulated firms authorised under FSMA and will extend to all investment firms, asset managers, consumer credit firms and mortgage and insurance brokers from 9 December 2019.
IA's role	IA should assess whether the firm complies with the Wholesale Market Codes in the following areas: • Oversight of governance, lines of accountability, skills and knowledge of staff and involvement of senior management. • Review of adherence to relevant codes and standards. • Review of controls over confirmation and settlement ensuring post-trade processes are efficient, transparent and risk-mitigating. • Review of the robustness of control and compliance frameworks and whether they effectively identify misconduct and/or divergence from market best practice.

6. Technology and Digital

Over the past few years, firms have been seeking new methods of creating value and actively leveraging digital, disruptive technologies and operating models. The digital era is complex, fast changing and brings a wealth of opportunities; however, operating in this digital world also presents new challenges. Digital technologies bring opportunities to increase efficiency, quality, customer experience and ultimately growth. However, they also bring a new set of risks and unlike traditional risks these emerge quickly, differ across technologies and can be hard to identify and control using traditional approaches.

IA can add significant value through involvement at the design stage to ensure benefits, such as cost reduction, improvement in customer experience, new revenue generation and regulatory compliance, are realised.

Taking into account the costly technology and digital issues that have arisen across financial services, IA also has a role to ensure the associated risks are properly understood and managed.

Our view of the change in IA focus from prior year to now:

	Technology and Digital hot topics for 2020	IA suggested areas of focus
6.1	Cyber Resilience	Significant increased focus of IA compared to 2018/19
6.2	Disruptive Technologies and Digitalisation	Significant increased focus of IA compared to 2018/19
6.3	Blockchain	Consistent focus of IA compared to 2018/19
6.4	Cloud Governance and Security	Significant increased focus of IA compared to 2018/19
6.5	Data Privacy and GDPR	Consistent focus of IA compared to 2018/19

6.1 Cyber Resilience

Overview	Given the high-profile cyber incidents across financial services in recent years, coupled with the continuing regulatory interest in this area, we anticipate that demands and requirements for firms around cyber and cyber resilience will only increase. The Bank of England, PRA and FCA issued a joint Discussion Paper in 2018, returning the spotlight to operational and cyber resilience. The focus is on the development of a broader framework for firms, enhancing resilience stress testing and establishing strong impact tolerances and performance metrics. Financial services firms will be expected to set their own resilience tolerances (maximum downtime for instance), in line with a resilience baseline and taking into account inter-connectedness with other financial services firms.
IA's role	IA should apply a risk-lens to the cyber agenda, taking account of regulatory, senior management and board demands on assurance and challenge. Areas of IA focus should include: • Governance and senior manager accountability for cyber resilience. • The extent to which a holistic, enterprise-wide approach to cyber and operational resilience is employed, that can influence a 'resilience' culture in the firm and drive 'resilience-by-design', particularly when it comes to the technology environment. • The quality of data-based metrics to monitor disruption, performance against key indicators and tolerances by system/component.

6.2 Disruptive Technologies and Digitalisation

Overview	Disruptive technology and the era of digitalisation are here to stay. Technological advances and trends in advanced analytics, robotic process automation (RPA) and cognitive intelligence, including Artificial Intelligence (AI), are rapidly transforming firms. They are reshaping 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. Limited availability of the right quality and quantity of data, insufficient understanding of AI's inherent risks, a firm's culture and regulation can all act as barriers to widespread adoption of AI in firms. Although the regulation in this area remains in its infancy, there have been some recent developments. The EU Commission published the steps it is taking for "building trust in Artificial Intelligence", 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.
IA's role	The EU Commission's announcements highlight that the ethical dimension relating to disruptive, new technologies is increasingly becoming a priority and will need to become an integral part of firms' development. IA's role is two-fold. First is to ensure appropriate controls are being implemented to prevent and detect new and emerging risks. Second is to challenge how the key requirements are included within the Commission's announcement for trustworthy AI are integrated in both the solutions their firms are deploying, as well as those that are already in use. Specifically, IA's role should include consideration as to whether relevant policies, structures and frameworks are updated to incorporate AI-specific considerations, for example firms' Risk Management Frameworks (RMF), Risk Appetite Frameworks (RAF) and governance structures. IA's role could also include the review of input data, underlying algorithms, the use of output and checking whether firms' proposed AI strategies are aligned to business objectives.

6.3 Blockchain

Overview	Blockchain is a digital, decentralised, distributed ledger which secures (via encryption) and tracks digital transactions. 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. Blockchain remains in its infancy, but firms are increasingly testing its usage and its capability to support business change. Risks from the corporate use of Blockchain technologies can be: • Technology and operational risks – 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 the 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 – 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 – 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.
IA's role	IA's role will depend on the rate of adoption of Blockchain technology in their respective organisations. IA's role should remain a value-add and impactful through understanding the specific implementations of the Blockchain technology, upskilling the team to truly understand the emerging and existing risks that the technology is susceptible to and staying ahead of the curve. Its role as a trusted business adviser and in anticipating/evaluating newer risks to the organisation is once again key, as organisations 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, IA should be able to 'separate facts from fiction', provide a clear objective and timely assessment of the risks posed by Blockchain and the governance and controls implemented to mitigate them.

6.4 Cloud Governance and Security

Overview	Cloud adoption has seen a significant upward trajectory over the past few years, with the global public cloud market projected to grow 63% over the next three years. The transformational benefits, such as flexibility (pay-as-you-go), technological sophistication, cost and tax efficiency, customer empowerment, are undeniable and have fuelled 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. Despite the expansion and increased level of maturity in adoption, benefits and technology, using the cloud is not straightforward. Even though a large part of the IT function may be handed over to a cloud service provider (CSP) and with it, much of the operational burden, users still bear the ultimate risks and responsibility if things go wrong.
IA's role	While security at CSP level has noticeably matured and improved in recent years, a greater risk to security remains within the cloud user organisations' control for example, in the better management of access rights, the level of discipline applied to monitoring changes in configuration, etc. As such, the role of IA within these organisations is fundamental, providing assurance over the effectiveness of these controls. IA should consider the following in the scope of their review activities: • Cloud governance and strategy. • Cloud insider risk, communications and people retention post-cloud deployment. • Complexity of technology integration with legacy platforms, deployment impact across the technology estate, project assurance over transformational or integration initiatives and security controls. • Data privacy considerations, including the physical location of data as well as broader operational and compliance risks. • Implications of GDPR and complying with other national laws.

6.5 Data Privacy and GDPR

Overview	The General Data Protection Regulation (GDPR) came into force in May 2018. The regulation carries significant regulatory fines for breaches, of up to 4% global annual turnover or €20 million – whichever is greater. Significant fines have been levied to date by the Information Commissioner's Office (the UK supervisory authority).
IA's role	IA should consider the following in their scope: • Assess the implemented data protection policies, procedures and controls to comply with GDPR. • Evaluate the effectiveness of the implemented framework and controls in response to the GDPR requirements. • Deeper focus on high risk functions (e.g. incident management, marketing and any other functions handling large amount of personal data). • Assess the accountability framework and data processing taking place abroad.

7. Internal Audit Strategies

The business environment has changed in material ways and this demands innovation. Without applying new approaches, an Internal Audit function may not be well placed to cope with strategic and technological developments, unable to meet evolving stakeholder needs and ill-equipped to deal with emerging risks.

IA Strategies embraces innovative approaches that helps keep the function ahead of developments.

Internal Audit Strategies

7.1 Internal Audit 3.0

Overview	As financial services firms move into an increasingly technology-driven, innovation-oriented and disruptive future, it is only right that we also ask what is the future of internal audit. For the most part, despite ongoing efforts to meet stakeholders' growing list of needs, the answer is: playing catch-up. A common theme in this publication across the past couple of years has been the need for Internal Audit to adopt new tools and techniques and to develop capabilities needed to effectively respond to today's challenges. However, it is equally important for Internal Audit to develop a coherent vision for both the profession and the function. Such a vision is essential in order to drive needed changes and prioritise initiatives for the function and the firm as a whole. Through consultation with Audit Committee chairs, Executives, Heads of Internal Audit and audit teams, we have developed a blueprint which aims to clarify the expectations of Internal Audit, codifying the most important components which is Internal Audit 3.0 (IA3.0). IA3.0 is Deloitte's view of the next generation of Internal Audit. It is intended to act as a guide, focusing a function so that it is attuned to the challenges of emerging risk, new technologies, innovation and disruption and able to fully assist in safeguarding processes and assets as management pursues new methods of creating and delivering value.
IA's role	IA3.0 embraces innovative approaches that help keep the function ahead of developments. Innovation positions Internal Audit to anticipate and then respond effectively to stakeholder needs and equips the internal auditors to address emerging risks in a helpful and impactful manner. IA should consider: • Readily adopting various methods and tools such as Scrum and Kanban to 'do' Agile Internal Audit. IA also need to create an environment in which Agile can thrive. • Automating core processes, using a combination of analytics and robotics in order to provide ongoing assurance, may be expensive. Where possible, IA can consider leveraging existing automation projects within the business. • The internal audit function of the future, which needs a vastly different set of skills and capabilities to those of yesterday. • Communicating clearly with its stakeholders to ensure they understand planned changes.

7.2 Auditing Strategic Change

Overview	A number of financial services firms are undertaking large-scale transformational change, in particular digital transformation. Transaction activity in the market is also prevalent, including through both traditional deal activity and Fintech acquisitions. Strategic change creates uncertainty, complexity and creates or increases risk, for example: • Risk that strategic objectives are not met/undefined as a result of poor decision making. • Heightened operational risk due to process and personnel changes. • Risk of cost overruns and non-delivery. • Risk that normal change management protocols are circumvented. Success or failure of strategic change can have significant operational, financial, reputational and regulatory impacts.
IA's role	IA can help a firm to achieve its objectives during the organisational change process by providing independent and objective assurance that risks are identified, assessed and managed. IA activity evaluates risk exposures relating to the firm's governance, operations and information systems. Specifically, IA should consider: • The viability of the organisational change and ability to deliver value. • The ability of the programme to deliver to the agreed timeframes and outcomes, following compliant project management disciplines. • Whether the programme appropriately manages and mitigates operational, regulatory and financial risk. • Whether the programme provides a suitable solution for the needs of impacted stakeholders.

Contacts

	**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.u
	**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 William**	Partner, Regions (Scotland)	0131 535 7463	stephenwilliams@deloitte.co.uk