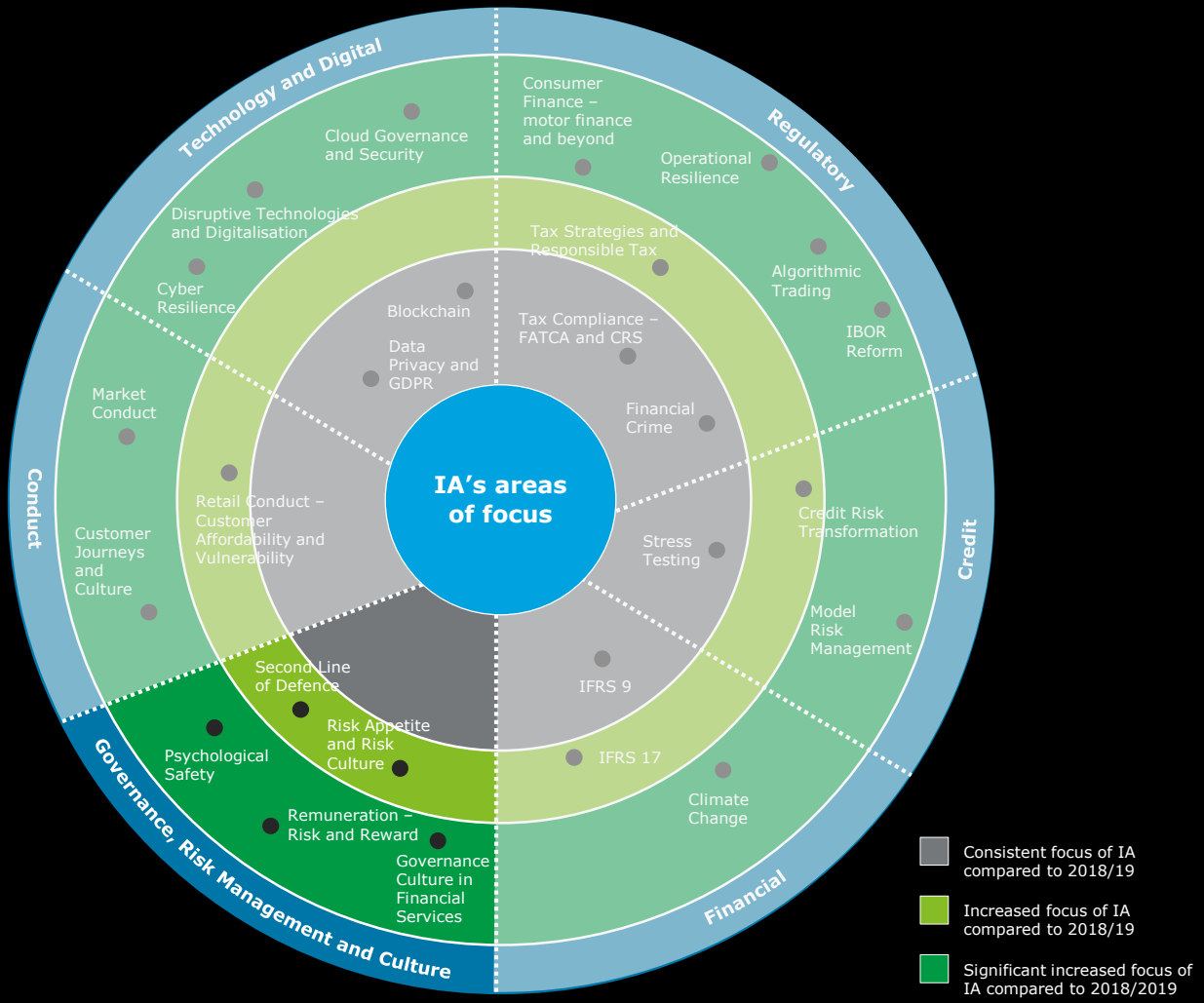
Deloitte.

Financial Services Internal Audit

Planning Priorities 2020 – Governance, Risk Management and Culture Hot Topics

Introduction

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 in the UK. There is an increased focus on the roles and responsibilities of the second line of defence, healthy cultures and psychological safety at the work place and the use of remuneration structures to encourage ethical behaviour towards customers and the financial market.



Contents

Key Industry Icons

Banking and Capital Markets

Insurance

Investment and Private Equity

4.1 Governance Culture in Financial Services

Why is it important?

The Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) frequently view the robustness and effectiveness of governance frameworks as the foundation of an established business that manages risk and complies with regulation. Corporate governance arrangements and the culture they promote and support are crucial to a firm's regulatory compliance, as well as the long-term sustainable success of the firm. A lack of robust governance arrangements that clearly articulate the culture of the firm can lead to the risk of behaviours that result in poor business and customer outcomes or regulatory breaches. There are a number of areas relating to Senior Managers and Certification Regime (SMCR) that firms should continue to focus on such as clearly defining responsibilities and articulating the delineation between individuals' responsibilities, specifically in areas such as technology and operations that impact all areas of the business; documenting reasonable steps that are taken in a consistent and practical way; and ensuring that Fit and Proper assessments are robust and adequately documented.

What's new?

The PRA's Business Plan includes evaluation of compliance with SMCR as a key element of their 2019/20 supervisory plan, and therefore firms should be considering how they have obtained assurance that their SMCR framework is in compliance with the regulation.

The importance of culture to the PRA is highlighted in SMCR through the inclusion of two specific Prescribed Responsibilities:

- Leading the development of the firm's culture by the governing body as a whole (must be allocated to an independent non-executive).
- Overseeing the adoption of the Firm's culture in the day–to–day management of the Firm (must be allocated to an Executive Director).

The Hayne Royal Commission also challenges all financial services' firms to look again at the way in which they govern themselves, in particular at how they perform their duties, take accountability, and effect real change.

What should Internal Audit be doing?

Area of focus	Description
SMCR – Senior Management Function	Review key elements for the Senior Management Function: • Senior Management Function ("SMF") allocation, the prescribed responsibilities, and the appropriateness of the allocation and whether there are any gaps with regulatory expectations. • Assess whether SMFs have produced handover documents.
SMCR – general	Review key elements of the SMCR regime: • Identify whether SMCR related policies have been embedded. • Assess the awareness of individual accountability and responsibilities through Statements of Responsibilities and interviews and review fit and proper processes as part of the wider recruitment process. • Assess training processes to support conduct rules implementation.
Corporate Governance (including Board effectiveness)	Review the corporate governance activities, focusing on the design and operational effectiveness of key controls, including reviewing: • The corporate governance structure and framework, including the composition, tenure and activities of the Board and Board committees and against relevant regulations. • Key documentation, including the corporate governance policies and procedures to ensure they support the overall culture and strategy. • Oversight and accountability case studies of decision-making.

4.1 Governance Culture in Financial Services

Are there any potential challenges?

Challenge	Description
Auditability – assessment of culture	Internal Audit must ensure that the assessment of culture is clearly defined in the audit plan.
Senior stakeholders	There is a risk of delay to the audit progress due to the seniority and availability of interviewees. The interview schedule should be compiled and meetings arranged as early as possible.
Timing	For Board Effectiveness reviews, there is a risk that a Board or Board Committee meeting may not be held within the audit timeline. This should be considered as part of planning if Board observation is one of the procedures planned.

What Internal Audit skills are required?

- Regulatory knowledge – Corporate Governance frameworks should be reviewed against the relevant regulatory standards (e.g. the Financial Reporting Council Guidance on Board Effectiveness and the PRA Supervisory Statement 5/16) to address the risk of a regulatory breach.
- Subject Matter Expert knowledge on the regulatory application process for SMCR and its components.
- Stakeholder management – due to the seniority of the stakeholders involved in a corporate governance review, these audits tend to require a higher input from senior managers within internal audit.

What's next?

- Individual Accountability will continue to be a theme for the regulator and is increasingly used as the regime to underpin other priorities.
- Firms should continue working on their SMCR, especially as regulatory scrutiny on firms' governance models through the SMCR lens is expected.
- The regulators will interview financial service firms' Senior Managers more frequently and therefore awareness and execution of Senior Manager roles and responsibilities is critical.
- The regulator will execute a stronger focus on Board culture, diversity and challenge.

Find out more

- https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-new-era-actions-royal-commission-130219.pdf
- https://www2.deloitte.com/uk/en/pages/audit/articles/our-governance-library.html

Deloitte contacts

Henry Hofman
Senior Manager
hhofman@Deloitte.co.uk

Chris Lane
Manager
crlane@deloitte.co.uk

4.2 Second Line of Defence

Why is it important?

The FCA reiterated the importance of effective governance within its 2019/20 Business Plan; *'We will seek to deliver protection for consumers through a continued focus on the culture and governance of the firms we regulate'* further adding *'Good governance, which enables effective oversight of decision-making, is critical for reducing potential harm to consumers or markets.'* A governance framework demonstrating appropriate three lines of defence responsibilities supports effective governance.

What's new?

The regulator continues to focus on the culture and governance within firms through the three lines of defence. The FCA is especially focused on the second line of defence risk management and compliance roles and responsibilities and how they are positioned and executed through firms' governance frameworks.

What should Internal Audit be doing?

Area of focus	Description
Segregation of roles and responsibilities, and culture	Assess roles and responsibilities for risk and control across the first and second lines of defence taking into account the risk structures and resources (considering both capability and capacity). Through consideration of roles and responsibilities Internal Audit can ascertain whether risk culture is perceived to be effective.
Demonstration of influence	Assess whether outputs from the second line functions (Risk and Compliance) are considered in the organisation and utilised in day-to-day decision-making process. Consideration should be given to whether appropriate risk-related governance committees within the organisation receive adequate management information from the second line functions in order to support decision-making.
Effective oversight of emerging industry issues/ regulatory concerns	Assess whether second line functions are sufficiently future facing and making early consideration of emerging issues and regulatory focus areas.

4.2 Second Line of Defence

Are there any potential challenges?

Challenge	Description
Clarity across the Lines of Defence	Misinterpretation of the three lines of defence model may lead to blurring of lines of responsibility. These challenges may be more prevalent for firms with less well-established risk management frameworks.
Reliance on Third Line Oversight	Second-line functions may over-rely on Internal Audit to 'plug the gaps' in second line monitoring.
Reluctance to hand off to the First Line	Second line may undertake first line activities due to a perceived (or material) risk of lack of capability or capacity within the first line.
Technical Expertise	Internal Audit should consider whether there is the in-house skillset and knowledge to review and assess specialist areas such as Financial Crime.

What Internal Audit skills are required?

- An understanding of the key regulatory requirements and best practice governance framework and the embedded governance framework within the firm.
- Internal Audit should be mindful of proportionality when considering governance and second line arrangements, especially in smaller, less complex organisations and those with low risk business plans.

What's next?

- Expansion of Senior Management and Certification Regime to all FCA Regulated Firms by December 2019. This will require firms to clearly establish the individual accountability of Second Line functions' senior managers so that consumers are treated fairly and market integrity is enhanced.

Find out more

- https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf
- https://blogs.deloitte.co.uk/financialservices/2019/05/fca-business-plan-201920-continuity-prevails-but-the-fca-also-looks-to-the-future-of-regulation-and-.html

Deloitte contacts

Lyndsey Fallon
Partner
lfallon@deloitte.co.uk

Alastair McGeorge
Senior Manager
amcgeorge@deloitte.co.uk

4.3 Risk Appetite and Risk Culture

Why is it important?

The FCA continues to focus on individual responsibility and accountability within financial services, and the extension of the Senior Managers and Certification Regime to all firms exemplifies this. The FCA wishes to promote healthy cultures within firms, which in turn should have the leadership capability to create and maintain them. It is important to align the risk appetite of firms with their risk culture to achieve business purpose, strategy, objectives, reducing 'blow-ups' and risk appetite and compliance breaches. Additionally, there is a need to ensure Non-Executive Directors challenge Executive Directors on adherence to risk appetite and that these are clearly documented in the Operational Risk Self-Assessment to promote good decision making.

What's new?

The FCA expects firms in the next year to demonstrate awareness of culture, and take steps to address any issues in their business practices.

While assessing the risk culture, the key points to consider are:

- Measures for the quality and embedding of the risk management and control approaches.
- Monitoring change initiatives; e.g. digital and technological disruption.
- Remuneration Committees need to consider Risk Intelligent and Ethical Culture considerations.

What should Internal Audit be doing?

Area of focus	Description
Audit plan – culture	Use culture profiles across the firms (vertical and horizontal demographics) to identify high risk areas for the audit plan.
Conflicts of Interest	Assess controls in place to manage any conflicts of interest within commercial arrangements which may drive in appropriate behaviour, and that customer interests are protected.
Culture/Risk Appetite Assessment	A focused review of the culture indicators within the business, and understanding what the target state is for culture and how it is embedded into strategy, governance and how this is measured/monitored through a risk appetite compliance assessment. If this has been previously identified by Internal Audit, focus should be on monitoring continual adherence to culture indicators.
Ongoing assessment of cultural indicators	Consider whether or not cultural indicators can be embedded into assurance work, with reporting provided via final internal audit reports and also tracked through Audit Committee reporting.
Operational Risk Self-Assessment	Review the Operational Risk Self-Assessment to ensure that Non-Executive Directors have challenged the Executive Directors on adherence to risk appetite.

4.3 Risk Appetite and Risk Culture

Are there any potential challenges?

Challenge	Description
Timing	Culture is ever present within a firm, and can shift without warning. Consider other influencers on culture such as structural changes, job security, negative press, Brexit etc. These may all account for variations in culture. Consideration should be made to continual monitoring to ensure trends can be tracked and other influences discounted.
Breadth	As a theme, Culture is far-reaching and even the reviews on previous slide could be expansive. Remuneration and incentives affects all the employees, and can manifest in different ways depending on audit area under review. Consider breaking into a framework/policy-based review to assess the strategic approach and tone to culture before selecting high-risk components such as sales activity.
Individuals	At a senior level, cultural drivers become less focused on processes and frameworks and more focused on individual behaviours e.g. senior management setting an appropriate tone and leading by example. Whilst Internal Audit should not shy away from assessing senior management (particularly with SMCR), this should be planned carefully in terms of timing and also seniority of the auditor.

What Internal Audit skills are required?

- An understanding of good practice in terms of FCA Training and Competency requirements.
- An appreciation of strategic and commercial drivers within a business, including revenue streams and business models, which may impact culture.
- An understanding of remuneration practices, and in some cases regulatory requirements, across products and services provided by the firm.
- An understanding of good practices with regards to governance, control and oversight of key cultural drivers. This will vary across firms and business areas.

What's next?

The FCA have acknowledged that changes to risk management and the protection of customers cannot come through changes to regulation alone and that firms should look to embrace accountability and responsibility. To that end, it should be expected that in conjunction with the extension of SMCR, cultural influences and drivers will remain a key consideration by regulators. As a result, Internal Audit should expect requests from the Audit Committee to challenge the firm's journey towards a well-embedded risk culture. This challenge may extend to assessing the Board itself.

Find out more

- https://blogs.deloitte.co.uk/financialservices/2019/05/fca-business-plan-201920-continuity-prevails-but-the-fca-also-looks-to-the-future-of-regulation-and-.html

Deloitte contacts

Stephen Gould
Director
stgould@Deloitte.co.uk

Alastair McGeorge
Senior Manager
amcgeorge@deloitte.co.uk

4.4 Psychological Safety

Why is it important?

Psychological safety is a feeling perceived within a conducive and healthy 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.

In December 2018, the FCA conducted its first CultureSprint on creating a speak up, listen up culture in financial services. FCA considers this cultural shift particularly important within Financial Services where a lack of psychological safety prevents employees from pursuing the best customer outcomes in the face of traditional behaviours and incentive structures.

What's new?

The FCA considers psychological safety as a critical element in their focus around Culture at workplaces. There is heightened focus on the risks associated with psychological safety including:

- Operational Risk: Undetected poor behaviours leading to poor customer outcomes.
- Reputational Risk: Damage to firm's reputation and integrity.
- Compliance/Conduct Risk: Increased risk-taking leading to higher compliance breaches and operational losses.
- Regulatory Risk: Firm's inability to comply with regulator's expectations of creating a risk intelligent culture.

What should Internal Audit be doing?

Area of focus	Description
Tone at the top	Review the tone at the top, including seeking evidence to demonstrate senior management are promoting a culture of psychological safety.
Governance	Review the governance and acceptance of formal decision-making processes with respect to the culture in the firm.
Understanding Employees	Hold structured interviews with employees at various levels to better understand the incentives and their current state capabilities as part of audit activities.
Assessment of psychological activities	Assess the design and operating effectiveness of initiatives and programs in the firm that promote a psychologically safe environment, particularly with regards to risk and controls. For example, assessing the effectiveness of speak-up and whistle-blowing programs, or whether governance forums effectively support management issues and listening to suggestions.
Reporting on psychological safety	Opine on psychological safety through assessing stakeholder behaviours observed during audits, audit findings and whether they support psychological safety.

4.4 Psychological Safety

Are there any potential challenges?

Challenge	Description
Assessing firm culture	Identifying drivers of behaviour that help assess firm culture and current state of psychological safety experienced by teams can be challenging.
Measuring psychological safety	Identifying solutions and indicators to measure psychological safety and produce Management Information is complex.
Eliminating deterrents to psychological safety	Promoting a 'Speak Up, Listen Up' culture should not impact employee bonus and incentive structure.
Behavioural Science Principles	Understanding the application of behavioural science principles in promoting psychological safety at workplaces is important.

What's next?

- An increased focus from the regulators and Senior Leadership to promote psychological safety at workplaces is expected.
- Internal Audit should leverage the concepts of psychological safety when commenting on culture in Internal Audit reports and Audit Committee papers. In the past, teams have found it challenging to talk about culture explicitly. However, increased focus from FCA on psychological safety provides Internal Audit teams with the means to opine on cultural observations.
- Internal Audit should be willing to challenge themselves as to whether there is a psychologically safe environment within Internal Audit, recognising that continuous improvement is a core principle of the IIA Standards, and enhancing psychological safety in the workplace is key to support this.

What Internal Audit skills are required?

- Internal Audit will need to involve cultural and behavioural subject matter experts and financial services' practitioners to provide a view on this rapidly evolving area within Financial Services.
- Involvement of subject matter experts to identify solutions/ indicators that help focus on assessing and measuring psychological safety amongst the employees and to produce MI.
- An holistic approach to compare and conclude on current state of psychological safety experienced in the organisation by drawing on various audits conducted in the year and to report to Audit Committees.

Find out more

- https://www.fca.org.uk/culture-and-governance/psychological-safety

Deloitte contacts

Matt Cox
Partner
macox@deloitte.co.uk

Manan Shah
Manager
mananshah@deloitte.co.uk

4.5 Remuneration – Risk and Reward

Why is it important?

In recent years, the regulatory and governance framework in financial services' organisations has become increasingly complex. A key area of focus has been in the area of remuneration structures, policies and processes where there has been a significant amount of regulatory change.

An example of this is in the insurance industry where the Insurance Distribution Directive (IDD) is now fully applicable. Remuneration is a key part of the IDD, which aims to enhance consumer protection when buying insurance and to support competition between insurance distributors.

What's new?

- An annual remuneration implementation review is included within the EIOPA guidelines for insurers under Solvency II. These Remuneration Codes require that "*a firm must ensure that the implementation of the remuneration policy is, at least annually, subject to central and independent internal review for compliance with policies and procedures for remuneration adopted by the governing body in its supervisory function*".
- The IDD is in full effect, which includes the change in IDD requirements for remuneration of staff including commission structures.
- The FCA is focused on remuneration structures and approaches 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.

What should Internal Audit be doing?

Area of focus	Description
Design	Review current remuneration policies, governance and disclosure to ascertain whether they are compliant with the regulatory framework: • Remuneration policies and variables (such as new hires, leavers, variable pay). • Governance (Remuneration Committee and broader Reward governance, including year-end process). • Remuneration disclosures (Directors remuneration report and Pillar 3).
Implementation	Test implementation of remuneration processes and procedures underpinning the remuneration policy to ensure they are robust and effective: • Remuneration process and procedures. • Decision-making framework. • Spot check of systems and outputs.
Future state	Consider how the firm is adapting to future regulatory requirements via review of the firm's readiness for future regulatory changes in reward.
Reward structures	Assess the Remuneration and Incentive arrangements across all parts of the business to ensure they are effective in encouraging a customer–centric culture. Specific focus should be paid to areas of the business where commission-based arrangements influence reward.

4.5 Remuneration – Risk and Reward

Are there any potential challenges?

Challenge	Description
Key themes of remuneration regulation	Regulations can be complex and continue to evolve. Internal Audit should ensure it understands the applicable rules and guidelines.
Remuneration committee and governance framework	Measuring effectiveness of the remuneration committee and remuneration governance framework can be challenging, Internal Audit should attend and observe governance meetings.
Disclosure	There are complex remuneration disclosure requirements in the directors remuneration report and Pillar 3. Internal Audit should ensure the review is performed on a timely basis, taking account of reporting deadlines.

What Internal Audit skills are required?

- Regulatory knowledge – Governance frameworks for remuneration should be reviewed against the relevant regulatory standards (e.g. the EIOPA guidelines for insurers under Solvency II and IDD) to address the risk of a regulatory breach.
- Knowledge of the regulatory application process covering remuneration frameworks for remuneration staff, including commission structures.
- Stakeholder management – senior stakeholders are involved in the development, implementation and execution of the Governance framework for remuneration and therefore these audits require auditors with suitable experience, skills and gravitas within Internal Audit.

What's next?

Organisations should be planning annual reviews of their remuneration policies, processes and implementation in light of the remuneration regulatory requirements.

Internal Audit should be planning to assess the rigour and robustness of this annual review where it is being performed by another function in the organisation. If required, Internal Audit may have to plan to undertake the annual review themselves.

Whichever role Internal Audit plays, they will need an approach that includes financial services regulation and reward specialists as this is a rapidly evolving area.

Find out more

- https://www.fca.org.uk/firms/insurance-distribution-directive

Deloitte contacts

Matt Cox
Partner
macox@deloitte.co.uk

Ed Thomas
Director
edathomas@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.