Building trust
2017 planning priorities for internal audit in financial services
## Contents

### Section one – outlooks

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory outlook</td>
<td>06</td>
</tr>
<tr>
<td>Retail Banking outlook</td>
<td>07</td>
</tr>
<tr>
<td>Capital Markets outlook</td>
<td>08</td>
</tr>
<tr>
<td>Insurance outlook</td>
<td>09</td>
</tr>
<tr>
<td>Investment Management outlook</td>
<td>10</td>
</tr>
</tbody>
</table>

### Section two – planning priorities

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Leadership</td>
<td>12</td>
</tr>
<tr>
<td>Risk Management</td>
<td>16</td>
</tr>
<tr>
<td>Regulatory Matters</td>
<td>20</td>
</tr>
<tr>
<td>Capital and Liquidity</td>
<td>31</td>
</tr>
<tr>
<td>Operations and IT</td>
<td>34</td>
</tr>
<tr>
<td>Accounting and tax</td>
<td>40</td>
</tr>
</tbody>
</table>

- **Building trust**: 2017 planning priorities for internal audit in financial services
- **Regulatory**: Embedding of risk management frameworks, Insurance risk pricing for cyber, Coverholder audits
- **Retail Banking**: BCBS 239, Conflicts of interest, MiFID II, Financial crime Conduct
- **Capital Markets**: Bank capital Solvency II
- **Insurance**: Operational resilience Assurance over third party management
- **Investment Management**: Project management Cyber Data Management and Governance Digitisation
- **Business Leadership**: Common reporting standards IFRS 9 IFRS 15 Qualified intermediaries and 871(m)
- **Risk**: Non-financial reporting frameworks
- **Regulatory Matters**: Corporate criminal penalties of tax evasion
Introduction

In an era of continued challenge around conduct and behaviour for firms, regulators and Boards are more aware of the issues and prepared to act. Customers and clients continue to expect more from the industry with work well progressed on topics such as Culture, Conduct or Conflicts of Interests.

This leaves a critical question for Internal Audit functions to address – how does their work provide confidence in the conduct and behaviour of firms, and ultimately help build trust with customers and clients? Are they focussed on the priorities that matter?

In addition we should expect market disruption, innovation and changing business models to put pressure on Internal Audit functions. The expectations on Internal Audit to cover the basics while adding more insight and value – being a genuine partner and critical friend – continue to grow. Many organisations are seeking to enhance growth and returns to build market share or access new technologies through acquisition, development into new markets or products, or partnerships to access talent. This adds pressure on Internal Audit to have a credible opinion on topics which in some cases didn’t exist a year ago. Making an impact is becoming more challenging.

So in this year’s publication we have developed the format from previous editions to help functions make this impact:

- Outlooks have been included covering the economic and regulatory changes as well as key market developments into 2017. We hope these add context to the financial services landscape that organisations will be facing to help Internal Audit functions focus on what truly matters.

- As we highlighted in our recent global survey of Chief Internal Auditors “Internal Audit at a crossroads – evolution or irrelevance” there remain a number of important challenges for Internal Audit functions. Most expect their organisations and functions to change substantially in the next few years yet lack the impact and influence they desire. There remain gaps in certain skills including analytics and IT, and methods of effective communication. While stakeholders expect more forward-looking insight around risk, strategy and business performance the expectation on Internal Audit to make an impact is now.

- Within each planning priority we have tried to differentiate the impacts on different sectors within financial services, so depending where your organisation is positioned that planning priority provides more tailored impacts.

This publication provides you with our thinking and we hope it proves useful as you plan and prioritise for 2017.
**Building trust** | 2017 planning priorities for internal audit in financial services

---

**Sector outlooks (part one)**

**Regulatory**  
Expectations continue to evolve – strong ethics, culture and accountability being as important as financial resilience.

**Retail Banking**  
Competitive advantage is being eroded with new analytical capabilities and innovative business models driving change. Growth will be focussed on the digital customer and tech-enabled disruption.

**Capital Markets**  
The use of high frequency, electronic and algorithmic trading practices increases operational risk – internal audit needs to ensure close interaction on this and innovative technology such as blockchain.

**Insurance**  
Insurers are responding to new market entrants through digital investments, increased outsourcing, optimising the use of specialists as well as accessing new markets.

**Investment Management**  
Cognitive technologies and automation enable the targeting of new investor segments with lower cost and higher customisation with tech-enabled disruption.

---

**Planning priorities (part two)**

**Business leadership**  
Culture and governance moved to top of regulator and stakeholder agendas.

**Risk management**  
Are you clear on the continued emphasis on risk management frameworks, and the impact on Solvency II, BCBS and cost?

**Regulatory matters**  
Risk data aggregation and reporting, conduct, conflicts of interests, Investors protection and financial crime are considered as some of the highest regulatory priorities for the coming year.

**Capital and Liquidity**  
Have you understood the impact of Solvency II on Capital Markets, Insurers and Fund Managers? An expectations for ICAAP and ILAAP reviews?

**Operations and IT**  
87% of respondents have faced a disruptive incident with 3rd parties in the last 2-3 years.

**Accounting and tax**  
CRS establishes obligations for verifying account holders tax residency and reporting information on reportable persons.
Section one – outlooks
Building trust | 2017 planning priorities for internal audit in financial services
Regulatory outlook

Regulatory expectations continue to evolve and expand. Regulatory attention has in most instances moved beyond the planning phase and is now focused on implementation. Strong ethics, culture, and accountability at every level of the organisation are now as important as financial resilience.

New regulatory requirements and expectations across a range of conduct and prudential topics that have recently come into effect include MiFID II/Markets in Financial Instruments (MiFIR), and Basel Committee on Banking Supervision (BCBS) 239, as well as requirements tackling financial crime and conflicts of interest, amongst others.

The European Commission’s report on how market liquidity can be improved, the potential impact of reforms and market developments is also to be published. The report and policy proposals are expected to be published by The Financial Stability Board (FSB) on the need for additional prefunded financial resources and liquidity arrangements for Central Counterparties (CCPs). This is expected to be accompanied by standards and guidance on CCP resolution planning, tools and the cross-border coordination and recognition of resolution decisions.

Additionally, a particular area of supervisory emphasis currently is each institution’s ability to respond to shocks or crises. The current list of possible risks is long with consequences for macroeconomic and financial market instability and dislocations. These put the spotlight on IT infrastructure, contingency planning and stress testing, amongst others.

Some banks have exited markets and changed how they participate in other markets, often leading to an influx of non-bank financial companies. This shift is prompting regulators to examine how regulatory requirements need to adapt to accommodate and respond to new entrants, and the new risks to the overall stability of the financial system they bring.

When tackling regulatory change, many organisations have traditionally operated reactively, only making changes in response to a particular regulatory deadline, supervisory direction or other type of regulatory pressure. However, increasingly organisations have started to shift towards a more proactive stance, with a more strategic approach to managing regulatory change and by establishing stronger links to business strategy and engagement with the regulators.

A forward-looking regulatory strategy creates opportunities to better align regulatory responses with business objectives. It can also improve the efficiency of implementation. By identifying connection points between regulatory and business strategies – instead of managing regulatory strategy as a side activity – banks can discover ways to achieve common objectives more efficiently and align compliance activities with their broader organisational goals.

Building trust | 2017 planning priorities for internal audit in financial services
Retail Banking outlook

What retail banks should look out for in 2017?

Cost savings
Banks’ core competitive advantages are being eroded by technology. Specifically, technology enabled innovation, which leads to the rise of non-bank competition (e.g. fintechs – although this also impacts the insurance and investment management sectors) in areas such as payments. Additionally the proliferation of non-bank fintech organisations is disintermediating the traditional banking value-chain, which has historically been organisations largely owned or controlled by incumbent banks. This will make the fight to generate returns above the cost of capital particularly challenging.

Channels are key, particularly in terms of whether digital and non-proprietary distribution can reduce variable front-line costs, and whether increased straight through processing (STP) can help rationalise the middle and back office. New analytical capabilities may enable banks to optimise their client relationships through their branch networks, and enable them to exploit their unrivalled treasure-trove of data.

Managing innovation
Emerging business models are using new technology to re-invent key elements of FS, e.g. payments specialists and marketplace lenders. The danger is not that non-banks replicate the universal banking model but, rather, that by innovating around it in support of their own core business, they fundamentally undermine the traditional integrated bank business model.

Banks’ growth models and strategies should closely link to the digital customer and tech-enabled disruption. The question here is how banks can best “future proof” themselves at a time of considerable uncertainty and when shareholders are demanding a focus on cost efficiency. This is tied to how banks collaborate with fintechs including through investments and acquisitions of fintechs, as well as cultural points around employee incentives and capabilities. It also requires a framework to understand which areas are priorities for investment.
Capital Markets outlook

What capital market participants should look out for in 2017?

**Operational and conduct risks**
The use of high frequency, electronic and algorithmic trading practices within wholesale markets increases the susceptibility to operational risk events and poor conduct outcomes for clients. Often this is a result of historical programming development, IT issues, and weaknesses in governance. Whilst the global regulatory landscape is both comprehensive and complex, there is a growing regulatory expectation that firms demonstrate better compliance of electronic trading regulatory requirements. This has led to a greater focus within firms to have a common, homogenous approach that is applied in electronic algorithmic trading governance. This ensures best execution and compliance with Markets in Financial Instruments Regulation (MiFIR)/Markets in Financial Instruments (MiFID) II.

**Innovative technologies**
Many capital markets institutions are currently piloting and adopting innovative technologies, some of which are likely to have far-reaching consequences for their value chains, processing capabilities and control frameworks. Whilst many fintech, and especially blockchain initiatives are in early stages, the implications for internal audit functions are significant and will require close interaction to maintain strong business and technology controls.
Insurance outlook

Digital innovation
Many parts of the insurance industry now are either technology related or have technology as a key driver. Trends such as growth of peer-to-peer insurance, cyber insurance, gamification, aerial & digital imagery and customer adherence apps will have a larger role to play in future. Start-ups are emerging in the insurance sector with fresh, innovative and potentially popular business models. New peer-to-peer start-ups claim to be 80% cheaper than traditional policies, for instance.

Internet of Things and Big data
The growth of internet connected devices and sensors, which are projected to number 50 billion by 2020, is changing the insurance market. Through the use of low cost of sensors, improved communication and increased data processing power, the Internet of Things is fuelling the rapid growth in the availability of real-time or near-real-time information – a trend often referred to as ‘big data’. Insurers who can exploit this information to identify customers’ needs and risks and to support better pricing, underwriting and loss control will have a distinct competitive advantage over their peers.

Change in business models
Over the last five years, insurance business models have evolved significantly to embrace the digital age, often through an increased use of outsourcing and specialists. As such, insurance business models are exploiting growth opportunities, to meet ever-changing consumer needs. Similarly, delegated underwriting and claims handling firms are increasingly engaged, either to bring in specialist skills or access new markets globally.
Investment Management outlook

Investment managers are under growing pressure to provide better value-for-money products, and calling for a re-think of costs and cost structures.

Fintech offerings will provide investors and smaller firms greater customisation and sophistication in their investments, thus drive market innovation and potential for expansion.

Key considerations:

• How will the playing field be impacted by innovation-driven and other disruptions?

• Is a new segment of investors emerging, and if so, how do firms target them?

• What parts of the investment management value chain will be influenced first?

**Industry and Technology**

Scale and process advantages of established investment management players are diminishing over time. The playing field will level as firms of all sizes take advantage of emerging networks and platform-based services to lower cost, improve compliance, and focus on markets with true competitive advantage.

**Product and Customer**

Cognitive technologies and automation will enable the targeting of new investor segments through lower costs and increased customisation. Increased sophistication of robo-advice will alter distribution models, forcing fewer traditional advisers to move upmarket.

**Business and operations**

Strong above market performance history has helped traditional investment managers navigate headwinds ranging from slowing fund inflows to share gains by absolute return and passive strategies. Rising transparency, and consequent fee and margin pressure, remain.

Interest in managed services solutions to drive front and back office cost savings will accelerate, both in core trading and customer records management. Several big fund houses have joined forces in testing blockchain technology by cutting out intermediaries and reducing staff. It is also viewed that blockchain will likely be gradually adopted for reconciliation, clearing and settlement, which would increase accuracy and speed whilst decreasing costs.
Section two – planning priorities
Culture can be thought of as a system of values, beliefs and behaviours that influence how work gets done within an organisation.

Culture in financial services (FS) firms has moved towards the top of the agenda for regulators, investors and consumers in the wake of excessive risk-taking by some firms in the run-up to the financial crisis and a string of misconduct scandals. Despite this, there can be a tendency on the part of some in the industry to see culture as “someone else’s problem”.

Within FS, banks have so far received the biggest regulatory fines for misconduct and the greatest scrutiny of their culture. However, concerns about misconduct span all FS sectors and regulators are following suit.

While there are certain cultural characteristics that are generally considered to contribute to positive or negative outcomes, there is no single “good” culture. Each firm needs to articulate its own desired culture, consistent with its strategy and risk appetite. To be effective, a target culture statement needs to include both principles and specific, measurable behaviours. These desired behaviours can then be used to form the basis of a culture assessment.

Regardless of how strong or weak a firm’s culture is currently, culture needs to be understood and actively managed. If it is not, it can rapidly become a serious threat to the reputation and success of the firm. Data on culture alone is not sufficient – Management Information (MI) must include analysis that leads to action.

The following represent a number of important external impetuses regarding taking culture seriously:

- 2016 European Banking Authority (EBA) Consultation Paper on internal governance.
2013 FSB: “Guidance on Supervisory Interaction with Financial Institutions on Risk Culture”

2015 FSB: “Measures to Reduce Misconduct Risk”;

Standard & Poor’s: “Approach for assessing Enterprise Risk Management”;

Increasing stakeholder pressure: e.g. general public, media, politicians, shareholders – even Hollywood through “The Wolf of Wall Street”, “The Big Short” etc.

The following represent a number of important internal impetuses regarding taking culture seriously:

- Competitive advantage: reduces chances of significant setbacks and improves performance;
- “Glue”: for aligning strategy, succession plans, risk appetite, risk management and remuneration;

Demonstrating it is being taken seriously: active involvement by Boards, non-executive directors, Board Committees (Audit and Risk; Remuneration); and

Measuring it to strengthen it: Internal Audit audits; Risk Management oversight; HR guidance.

The impacts on each sector are considered consistent.

What can Internal Audit do to address this?
- Check that MI on culture is objective wherever possible, is drawn from a range of sources and contains evidence-based analysis and recommendations;
- Make sure that MI is supported by appropriate governance and capabilities, including people, processes and IT systems; and
- Carry out specific culture assessments or consider culture as part of their root cause analysis on all audits.
Governance is about effective delegation of authority. As the regulators call for clear accountability, organisations need to find a better way of allocating and cascading responsibilities with appropriate authority levels that are clearly documented and well understood. Specific applications worth exploring are in relation to group governance and management level governance. Legal entity structure optimisation and subsidiary governance will likely gain further momentum in the near future given the recent political developments.

There is a growing trend of interplay between the traditional concepts of risk management framework and delegated authorities. Completeness and cascade of the risk taxonomy and the way authorities are delegated may be critical to satisfy regulatory expectations.

What can Internal Audit do to address this?

- Examine whether the right management decisions are taken at the appropriate level with the right stakeholders around the table;
- Test whether there is sufficient evidence to document rationale and circumstances of the key decisions being taken;
- Assess whether Senior Managers delegate their responsibilities in a transparent and effective manner in compliance with their regulatory responsibilities;
- Test whether decisions and responsibilities of the executive committee are appropriately delegated within the firm and within the group; and
- Test whether subsidiary governance systems are in line with group governance frameworks and key decisions and approvals are appropriately delegated and escalated as needed.
Building trust | 2017 planning priorities for internal audit in financial services
A risk management framework is embedded when the organisation is risk intelligent. Specifically, when everyone understands the organisation’s approach (arrangements and design) to managing risk, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example.

The drivers for embedding risk management frameworks are increasing regulatory pressures, reduced operational loss exposures (such as fines and remediation costs from compliance breaches) and increasing competitive advantages deriving from informed management decisions.

What can Internal Audit do to address this?
- Awareness of ‘Risk Strategy’: Evaluate whether leaders, managers and the risk function know the risk strategy and how the framework's systems and risk function capabilities are targeted to evolve to enable the business strategy; and
- Risk intelligence or risk culture: Examine people’s perception of the risk management framework at all grades, geographies and business lines throughout the organisation, in proportion to everyone’s ‘day-to-day’ risk related activities.
What is the impact on Retail Banking and Capital Markets?
Retail Banking and Capital Markets firms are being prompted to reconsider their operational risk management frameworks. One being that BCBS has recently proposed replacing its current approach for operational risk capital calculation with a Standard Measurement Approach (SMA). The other being a growing number of banks are now seeking to combine their non-financial risk frameworks and deploy an integrated ‘Governance, Risk and Compliance’ (GRC) single system solution; instead of utilising different system solutions for each standalone non-financial risk frameworks.

What is the impact on Insurance?
In preparation for SII ‘go live’ on 1 January 2016, much time, money and effort was invested by insurers enhancing the design and implementation of their risk management frameworks. Post SII go live, the focus is on embedding the implemented frameworks so the insurer can truly see the full return on its investment.

What is the impact on Investment Management?
The obvious drivers for many IMs to seek to embed their risk management frameworks are to reduce their operating costs coupled with the urge for more effective risk management oversight and a control effectiveness agenda.

Building trust | 2017 planning priorities for internal audit in financial services
Insurance risk pricing for cyber

Cyber, as a class of business, is growing significantly in the commercial and specialty insurance market. There is also increasing pressure on insurers to widen terms and conditions in a number of lines of business, in order to provide cover for cyber exposures. Furthermore, there are also a large number of policies where coverage for cyber is not specifically included or excluded.

Cyber is a rapidly developing area of risk. In particular:

- **Aggregation**: the increasing frequency of cyber-attacks leads to increased potential for aggregation of exposures. It is important that insurers monitor these against their risk appetite.

- **Reserving**:
  - reserving uncertainty due to lack of claims experience, historical data and market benchmarks;
  - challenges with the evaluation and monitoring of cyber reserves due to the immaturity of cyber insurance mean that reliance on standard reserving techniques is less appropriate;
  - there is a threat of under-reserving given the continuing soft market conditions; and
  - the risk that claims are not being notified on a timely basis to insurers due to fear of reputational damage and therefore this increases the uncertainty in reserving.

- **Coverage**: coverage is dependent on the facts of the claim and the terms and conditions of the particular policy. If this is not clear to the cyber policyholder, there are potential conduct risks.

Insurance companies and Lloyd's of London syndicates need to understand the cyber risks they are writing, the aggregate risk they are exposed to, the market trends for cyber-crime, and assess that their reserves are sufficient to meet potential future liabilities.

**What can Internal Audit do to address this?**

- Include, typically as part of an Own Risk and Solvency Assessment (ORSA) or Risk Management audit, testing of the setting and monitoring of the insurer’s risk appetite for exposure to cyber-attack and reporting against that risk appetite to the Board; and

- Perform specific cyber underwriting audits, as a newer class of business, with scope areas including pricing, risk aggregation and exposure management, conduct risk and reserving.
Coverholder audits

There continues to be regulatory focus on how insurers oversee and control their underwriting and claims handling agents. Results of regulator's thematic reviews on delegated authorities found significant variations in the quality of insurer's oversight of outsourced functions.

This level of regulatory scrutiny is driving the need for higher quality coverholder audits to better demonstrate oversight and control, including being risk-based and proportionate, with clear evidence to support the results.

What can Internal Audit do to address this?

- Assess the effectiveness of the Delegated Authorities teams' risk-based oversight framework with respect to coverholders and claims handling agents, and the ability of the firm to robustly evidence the approach it has taken, standing up to regulatory scrutiny;

- Assess the quality of coverholder audits being performed, including adequacy of scoping, the quality of reporting and the rigour with which findings are being monitored and tracked to resolution; and

- Work closely with the Delegated Authorities team to avoid duplication of effort in auditing coverholder operations.
Regulatory Matters

The BCBS Principles for ‘Effective Risk Data Aggregation and Risk Reporting’ apply to Global Systemically Important Banks (G-SIB) (and Domestic Systematically Important Banks (D-SIB) three years after recognition) with the objective of improving each institution’s ability to manage their risks better through improved risk data aggregation capabilities and risk reporting practices. The principles cover:

- **Overarching governance and infrastructure** – banks should have in place a strong governance framework, risk data architecture and IT infrastructure (Principles 1 and 2);

- **Risk Data Aggregation** – banks should develop and maintain strong risk data aggregation capabilities so that risk management reports reflect the risks in a reliable way (Principle 3, 4, 5, 6);

- **Risk Reporting Practices** – risk reports based on risk data should be accurate, clear and complete. The reports should be presented timely to the appropriate decision-makers that allows for an appropriate response (Principles 7, 8, 9, 10 and 11); and

- **Supervisory review, tools and co-operation** – applicable to supervisors only, and covering review of compliance with the principles (Principles 12, 13 and 14).

Institutions which fail to demonstrate sufficient progress towards full compliance with the Principles (which became effective on 1 January 2016) will be subject to punitive actions imposed by Supervisors, such as additional Pillar 2 capital charges.

Ongoing independent validation of compliance (which should be considered separately from internal audit work) is a requirement of the Principles, and in addition, BCBS publication D348 stated that independent evaluation of compliance should be carried out (by either internal or external auditors).

**What can Internal Audit do to address this?**

- Assess the suitability of the bank’s Independent Validation framework design and operating model;

- Consider in the case of non-compliance at the implementation deadline, the robustness of remedial plans and the extent that these are agreeable to the bank’s Supervisor; and

- Carry out a project management audit of the firm’s programme to manage the implementation of the Principles to assess the speed and quality of the improvement in architecture and processes.
What is the impact across the FS sectors?

Compliance with the 11 principles was targeted for 1 January 2016 for G-SIBs, and D-SIBs are due to comply 3 years after recognition, with a list of EMEA D-SIBs having been published in March 2016.

Results from the latest progress review by the Basel Committee showed limited progress by firms, with challenges relating to the timeliness of reporting and the implementation of a robust IT infrastructure. In the document, the Basel Committee:

• Recommends the development of high quality infrastructure and improvements in automation.

• Required banks to submit a remediation plan in the case of non-compliance by 1 January 2016.

• Recognises the increase in senior management involvement in improving architecture and processes.

• Puts emphasis on an independent evaluation of compliance, either by internal or external audit teams.

The principle-based nature of BCBS 239 presents a challenge in itself, as banks need to interpret the requirements and demonstrate qualities such as “completeness,” “timeliness,” “adaptability” and “accuracy” which can have different meanings, and potentially different metrics, when applied to different risk types (e.g. credit, market and liquidity).

Specific industry considerations:

Retail Banking and Capital Markets

Whilst virtually all G-SIBs are active in these sectors, covering the mandated risk types (market, credit, liquidity and operational), it is likely that an ever larger population of regional players (D-SIBs) will be progressively requested to comply with the Principles.

Investment Management

Whilst pure investment management firms are not in scope for compliance with BCBS 239, the largest players have started targeting compliance with the Principles, understanding the benefits and the positive developments arising from better risk data quality and improved risk management.

Insurance

The insurance industry has been excluded at inception from the scope of BCBS 239. However, regulators in some countries (Canada being the prominent example) have requested the largest firms in the sector to align themselves to the standards required to G-SIBs. This trend is expected to continue, therefore internal audit departments in these firms should start targeting the review of compliance in their annual audit plans.
Managing conflicts of interest is a longstanding key focus area for the regulators, and it has imposed numerous fines on firms for inadequacies in this. Managing conflicts of interest fairly, both between the firm and its customers and between a customer and another client is enshrined in many regulations as a fundamental obligation on firms.

Recent publications by the regulators have shown that improvements are still required from firms across retail and wholesale markets. Many regulators' thematic reviews found deficiencies in the use and recording of hospitality, excessive payments to cover training, and that MiFID firms were not disclosing to clients the value of benefits provided such as training. Concerns with conflicts of interests have also been identified.

Moreover, under European requirements such as MiFID II and the Insurance Distribution Directive both of which are due to take effect in early 2018, there will be a greater emphasis on firms to prevent conflicts of interest, as opposed to managing them and disclosing them to clients.

Firms need to be mindful that further work may be needed to meet their current and expected regulatory requirements over conflicts of interest.

**What can Internal Audit do to address this?**

- Review the adequacy and effectiveness of the firm’s systems and controls framework for identifying, preventing and managing conflicts of interest to ensure fair customer outcomes; and

- Challenge the firm’s preparedness for relevant emerging regulations on conflicts of interest and inducements, for example, under MiFID II and the Insurance Distribution Directive.
What is the impact on Retail Banking?
Retail banking firms should pay attention to how their business models or practices could create conflicts of interests particularly between themselves and their customers. For example, are the products sold ‘in-house’ only or from other product providers too, and whether distribution agreements cause the potential for product bias. Considerations on this could include whether there are sales incentive schemes that might drive inappropriate behaviours leading to unfair customer outcomes or whether the appraisal process includes an appropriate balance of conduct risk/quality measures as well as sales performance.

What is the impact on Capital Markets?
Capital markets firms should continue to review and assess conflicts of interest inherent when issuing capital in the equity and debt markets, for example with regard to practices associated with the allocation of securities, underwriting practices, etc. More broadly, continuing to address the use of confidential information in the client facing and market making businesses through effective Chinese walls should remain a key part of the control environment.

What is the impact on Insurance?
Under the Insurance Distribution Directive, there will be a greater focus on preventing conflicts of interest, in addition to identifying and managing them. Considerations that could be taken into account include what arrangements are there between the insurer and intermediaries, including commission payments, profit share agreements, volume override agreements and claims management. Also, attention should be placed on arrangements over gifts and hospitality and other inducements.

What is the impact on Investment Management?
In addition to the considerations on conflicts of interest identification, prevention and disclosure, vertically integrated investment management firms (that provide product offerings as well as advice) should carefully examine their existing business models and have appropriate controls in place. This is particularly in relation to conflicts of interest risks with regard to client orders, best execution and handling client money.
With MiFID II due for implementation on 3 January 2018, firms should be well underway in their implementation programmes. MiFID II is the new EU regulation framework for firms who deal in financial instruments with clients. MiFID II has a number of potentially significant implications for firms, including dealing with technology changes, data challenges, and strategic decisions.

What is the impact on Retail Banking?
There are some changes to scope, with certain types of structured deposits being brought into scope of the requirements.

What is the impact on Capital Markets?
There are likely to be significant changes to both the market structure landscape, as well as internally within firms to existing processes and technology.

What is the impact on Investment Management?
Significant changes are abound, including a ban on portfolio managers receiving inducements which will impact the way that research is currently paid for.

What is the impact on Insurance?
There are limited implications for insurance undertakings. Again, the main impact will be for the investment management arms of the insurance undertakings.

What can Internal Audit do to address this?
• Confirm that appropriate governance arrangements on MiFID II are in place;
• Check the seniority of decision makers;
• Verify that there is sufficient consideration of potential linkages to other regulations;
• Assess the adequacy and maintenance of traceability and audit trails; and
• Assess the achievability of deadlines and progress for MiFID II implementation programmes.
Financial crime

The regulators unrelenting focus on financial crime continues, particularly in relation to anti-money laundering (AML).

Firms have been strongly encouraged to conduct assessments of the risks posed by their customers and institute sophisticated systems and controls which prevent financial crime.

What is the impact on Retail Banking and Capital Markets?
Retail banks are encouraged to have appropriate AML tools and technology in place to provide the functionality and automation required to identify and effectively manage AML risks.

What is the impact on Investment Management?
Fintech companies are making inroads into the wealth and investment management space, leading to digitization and altering aspects of the traditional model of client experience. While fintech companies may appear challenging for the investment management business model, there is an opportunity to leverage them for enhancing AML systems and controls.

What is the impact on Insurance?
In reaction to heightened regulatory pressure and scrutiny, the insurance sector is increasingly considering to allocate suitable resources to manage financial crime risks.
Conduct

Retail Conduct Risk
Poor retail conduct by firms and employees remains a common factor in many issues that have arisen since the financial crisis.

What can Internal Audit do to address this?
• Verify the risk and control framework supports the management of the firm’s conduct risks; and
• Test the key business controls that support the delivery of good outcomes for customers, clients and counterparties.

Wholesale Conduct Risk
Wholesale conduct risk represents the risk that the actions or inactions of regulated firms or their staff creates undue detriment to their clients or to the integrity of the market.

What can Internal Audit do to address this?
• Promote the testing of the alignment of inherent and residual wholesale conduct risk with the conduct risk appetite as expressed by the Board.

Applicable sectors
- Retail Banking
- Capital Markets
- Investment Management
- Insurance

Building trust | 2017 planning priorities for internal audit in financial services
What is the impact on Retail Banking?
MiFID II will increase the focus on digital distribution, but conduct risk concerns will remain a barrier to some innovation. Supervisory focus on consumer credit, credit cards and mortgages will continue, with the Regulators placing a high priority on affordability assessments and the fair treatment of vulnerable customers and those who are in arrears.

What is the impact on Insurance?
Regulators will continue their focus on sales of annuities. Rule changes may affect distribution with the implementation of MiFID II, seeking to provide consistency between MiFID II investment products and insurance investment products, and looks to implement the Insurance Distribution Directive.

What is the impact on Investment Managers?
The focus for investment managers will remain on having fair outcomes for clients in product design, distribution, execution and fee structuring.
Ongoing regulatory focus on wholesale market integrity and investor protection has resulted in continued supervisory attention on firms' governance and controls around order handling and client categorisation, on both the buy and sell side. The European Securities and Markets Authority sees delivery of best execution as a fundamental component to having market integrity and fair outcomes for clients.

Regulators have been undertaking some targeted supervisory visits which are likely to continue into 2017.

What can Internal Audit do to address this?

- Understand whether the scope of activities covered by the best execution obligations has been integrated into the business' controls, documented in its policies and procedures and is understood by the business via training requirements;
- Verify that effectively designed pre and post-trade monitoring systems are functioning appropriately and examine the related processes to assess whether the organisation is meeting its best execution obligations; and
- Assess whether accountability for best execution is clear and if responsibility for having that policies and arrangements are fit for purpose is taken.
Clarity of charges and fees on complex products will remain a focus area in capital markets and investment management. MiFID II establishes a new requirement for firms to disclose costs and charges associated with a client’s investment. For example, costs that may not typically be disclosed to clients today, such as transaction costs, will need to be disclosed in the future.

Firms need to be able to evidence fair outcomes for clients and increase price transparency, where information asymmetries create potential undue detriment to clients.

What is the impact on Capital Markets?
Complex and structured products should be subject to a robust internal pre-approval and review process so that charges and fees are communicated transparently, including formal signoffs from the front office, business development, marketing, compliance and legal.

What is the impact on Investment Management?
Annual management charges and on-going charges will need to be made subject to enhanced internal scrutiny within marketing materials and existing contractual arrangements.

What can Internal Audit do to address this?
• Ascertain that the design and fee structures for complex products are sufficiently correlated and are communicated transparently to the targeted client segment.
Building trust | 2017 planning priorities for internal audit in financial services
Capital and Liquidity

As part of the European Banking Authority’s Supervisory Review and Evaluation Process (SREP), banks and investment firms must internally review their capital and liquidity requirements via the Internal Capital Adequacy Assessment Process (ICAAP) and the Internal Liquidity Adequacy Assessment Process (ILAAP).

Banks should be looking to the guidance provided by the EBA and PRA when reviewing their ICAAPs & ILAAPs and preparing for SREP visits.

What can Internal Audit do to address this?

• Review the effectiveness of the key controls in the development of the ICAAP and ILAAP key processes, such as stress testing; and

• Substantively review the ICAAP and ILAAP documents themselves as well as management’s preparation for SREP visits, taking into account guidance provided by the EBA.
The journey toward the Solvency II (“SII”) capital reporting regime has been a long and arduous one for the insurance industry. Several years of hard work by insurers’ financial and regulatory reporting teams on their systems and processes to deliver the required public and private SII reporting have now come to a head and soon the industry will begin to see how regulators are using this information.

The approach to governance has been evolving as the processes and systems to report have now been tested through reporting in a live SII environment. The granularity and nature of the information requested by those charged with governance is likely to continue to change as the market begins to adapt to this new reporting basis and the expectations placed upon Directors by the regulators becomes clearer.

Whilst processes and systems have been built, it is clear that there is still much work to do in terms of documentation to make sure that insurers’ SII reporting stands up to external scrutiny. This will be made all the more difficult given the need for reporting speeds to increase as reporting teams move towards the end-state timetable, which is likely going to necessitate further process redesign. It is therefore crucial that insurers work with their second and third line functions to produce a process that is robust and will pass independent review.

**What can Internal Audit do to address this?**

- Include within their annual audit plans a review of the newly created governance processes, comparing management’s process against the regulators’ expectations;

- Think about how they can use the wealth of data that exists within the Solvency II, alongside that for other firms which is publicly available, to identify unusual trends or anomalies which they can use to focus their independent challenge; and

- Review the framework that lays down rules which permeate all aspects of an insurer’s risk management framework, including reviewing the firm’s comprehensive suite of reporting, both quantitative and qualitative.
What is the impact on Capital Markets?
Capital Markets are likely to take some time to fully understand this new reporting basis for insurers and learn how to interpret movements in key metrics to guide their investment decisions.

What is the impact on Insurance?
SII is not just about capital. Insurers are likely to expend a great deal of effort over the next few years optimising their capital positions under the new framework, as well as refining their management information and external reporting to deliver the information that both management and external stakeholders need.

What is the impact on Investment Management?
SII places greater data needs on insurers and asset data is no exception. Investment managers have already needed to adapt to provide insurers with the data they need to complete their reporting, and they will need to be cognisant of the fact that timeframes for the provision of data may begin to accelerate as insurers move towards end-state reporting.
Resilience is not just an organisation’s ability to prepare for, respond to, and recover from adverse circumstances but also to withstand such disruption, maintaining the availability and performance of services, and the IT that enables those services.

Organisations are facing increasing amounts of uncertainty and disruption, bringing both risks and opportunities, which more resilient organisations are better prepared to overcome and gain from. Regulators are asking how firms will be able to maintain client services in particular in controlling access management, managing change and managing service from IT vendors.

**What is the impact on Retail Banking?**
Resilience is critical wherever customers and regulators expect high availability of services. Resilient Retail Banking systems improve services to customers and reduce the risk of regulatory intervention.

**What is the impact on Capital Markets and Investment Management?**
Reliable, available and resilient systems are critical to maintaining an edge over competitors and liquidity in markets where quick response times and access to data underpins profitability.

**What is the impact on Insurance?**
Insurers need to be sure that their customers are not impacted by any IT disruption.

**What can Internal Audit do to address this?**
- Assess the organisation’s approach and risk appetite for resilience;
- Promote a resilience culture in each part of the organisation; and
- Confirm that IT availability planning truly aligns with business requirements.
Third party risk has become a regular board level agenda item as a result of growing global regulatory attention around the use and control of third parties for key business activities.

Organisations need to be able to demonstrate their actions taken to manage third party risk. In many cases there is limited oversight of the business wide approach to, and success of, third party risk management.

While organisations can outsource activities to third parties, they cannot outsource their risk. Inconsistency in approach and weak controls around third party risk management can result in significant financial, reputational or regulatory damage as well as missed opportunities.

Applicable sectors

- Retail Banking
- Capital Markets
- Investment Management
- Insurance

What is the impact across the FS sectors?

Regulators have clarified their expectations regarding third party risk management. Some key areas that organisations have struggled with so far include expectations that:

- All third party types need to be considered consistently, including inter-entity third parties. Often in the past, activities have been limited to vendors.

- There will be greater board level oversight, resulting in a need to enhance internal reporting processes and central visibility.

- Risk will be managed throughout the third party lifecycle. Many organisations are stronger in performing pre-contract due diligence than they are at managing the risk throughout the relationship.

What can Internal Audit do to address this?

- Perform a diagnostic maturity assessment of the organisation’s approach to third party risk management against good practice and regulatory requirements; and

- Assess compliance with existing third party risk management policies and procedures.
Constant change is the new reality with strategic transformation projects being a critical element of maintaining a sustainable business. Such initiatives place increasing demands on technology, necessitating large-scale projects to upgrade and replace aging legacy systems.

The success or failure of a project can have a substantial impact on reputation, business performance and the confidence of stakeholders.

Internal Audit play a vital role in project reviews and challenging management on how project execution risks are controlled.

What can Internal Audit do to address this?
- Consider not just adherence to project management frameworks, but also whether the project remains viable, compliant and aligned to the firm's strategy.
Organisations’ increasing reliance on third parties to provide business critical processes exposes them to unknown cyber security risks. Third party incidents can lead to critical data breaches and service interruptions, which can have severe reputational and/or financial impact.

There is an increasing expectation from regulators that organisations manage their cyber security risks effectively, which includes taking responsibility for third party risks.

The findings from Deloitte’s 2016 Global Survey on Third Party Governance and Risk Management, which had representation from 170 organisations across different sectors, found that 87.3% of respondents have faced a disruptive incident with third parties in the last 2-3 years. Embedding third party cyber risk programs allows firms to define and implement controls to manage this risk effectively, and help reduce potential financial, regulatory and reputational risk.

Where cyber risk is not managed, FS organisations are at risk of financial reporting errors, monetary losses, regulatory fines or penalties, breaches of sensitive customer data and service disruptions.

What can Internal Audit do to address this?

- Check that a comprehensive third-party risk assessment has been conducted, and use the ratings to develop the third party security audit plan;

- Review whether security standards have been adequately incorporated into third party contracts and include a “right to audit” clause; and

- Establish third party security risk reviews as part of an on-going internal audit plan.
Data Management and Governance

Data Management and Governance are the frameworks and systems in place to govern all of an organisation’s data assets and usage.

Recent and upcoming regulatory scrutiny (e.g. BCBS 239 and EU’s General Data Protection Regulation (GDPR)) and the changing data technology landscape mean that this is a key area of risk for organisations.

A number of key risks and impacts are associated with ineffective data management and governance, including regulatory non-compliance (e.g. BCBS 239, GDPR which have explicit data management and governance requirements), cost and operational impact associated with poor data quality (e.g. high volumes of manual Risk & Finance reporting adjustments) and inaccurate reporting impacting both business decisions and regulatory submissions.

What can Internal Audit do to address this?

- Understand the risks surrounding implementation of new data stores and management platforms; and
- Leverage both as analytics and the organisation’s consolidated data stores to drive more insightful and efficient internal audits/reviews.

What is the impact on Retail Banking, Insurance and Investment Management?

Under GDPR, new data privacy/protection activities are required which specifically link to compliance demands (e.g. a consumer’s “right to be forgotten”).

What is the impact on Capital Markets?

Some G-SIBs are now required to comply with BCBS 239, meaning that the regulatory risk is now more tangible.
The usage of social media and mobile platforms is growing and as a response, many FS organisations are investing heavily in digital transformation programmes to build or improve customer experiences. This has led to a firm’s Risk and Audit being asked to evolve their practices to promote a balance between digital innovation and good governance.

What is the impact on Retail Banking?
Retail banks are still at the forefront of digital governance in the FS industry and are expected to continue to lead in this space by helping shape best practice.

What is the impact on Capital Markets?
Digital brings speed and agility for capital markets. The use of electronic trading through digital channels is growing. The underlying (legacy) trading infrastructure may pose challenges to support this growth.

What is the impact on Insurance?
Selling and promoting insurance products through new digital channels will bring additional considerations, especially with the use of various parties such as agents and brokers who may have their own digital strategies.

What is the impact on Investment Management?
Investment managers are increasingly using alternative digital servicing models such as robo-advisors to offer services to clients. This has now come under the attention of the regulators with for instance the launch by the FCA of a robo-advice unit in 2016.

What can Internal Audit do to address this?
• Monitor regulatory requirements and guidance on digital technologies; and
• Interact with the business to check that controlling mechanisms are in place for digital through strategy, governance, policy, awareness and monitoring.
Accounting and tax

Common reporting standards

Tax authorities are continuing their commitment to implement the Organisation for Economic Co-operation and Development (OECD) Common Reporting Standard (CRS).

The measures establish obligations for businesses including identifying which group entities are financial institutions, verifying account holders’ tax residency and reporting information on reportable persons. The regulations also include provisions that can require financial institutions to notify their customers about CRS obligations, penalties and disclosure facilities.

The definition of a financial institution is drawn widely and includes banks, insurers, funds and certain investment entities (e.g. trusts and personal investment companies). There will also be an indirect impact on non-financial companies who will still need to comply with additional requests for information from financial institutions.

Under CRS, reporting volumes for FS firms will grow significantly driven by an increase in counterparty jurisdictions requiring information, expansion of the financial institution definition and a reduction in the exemptions for account holders (e.g. removal of thresholds and regularly traded exemptions). Additional complexity will also arise in monitoring which jurisdictions are treated as ‘participating’ under CRS. Some large jurisdictions, such as the US, are non-participating and investment entities located there may be treated as ‘passive’ with financial institutions required to look through to the underlying investors when conducting due diligence.

Overall, CRS builds on the previous work completed by financial institutions for US’ Foreign Account Tax Compliance Act (FATCA). However, the breadth of reportable persons adds a level of complexity that will likely test already stretched technology and teams.
What can Internal Audit do to address this?

- Review the operating model to confirm that adequate procedures are in place for CRS compliance and that sufficient resources and training are in place to support these;
- Review that IT systems are ready to handle the increased volume of reportable information; and
- Review the governance approach and check that evidence required for tax authority audits are sufficient and adequately maintained.

What is the impact on Retail Banking, Capital Markets and Investment Management?
The CRS will have an impact on a variety of the key processes and systems of a retail bank, including:

- Master data management – via the need to include foreign indicia;
- KYC/AML and due diligence – via the need to enhance systems to capture additional data;
- Regulatory reporting – via the need to adopt a jurisdiction-specific standard reporting and information exchange-model; and
- International transaction processing – via the need to identify certain payments and certain accounts.

What is the impact on Insurance?
The insurance sector is also likely to have the following impacts:

- Scope – under previous regimes, insurers benefited from exemptions that excluded reviewing the back-book of business, these are not available under CRS;
- Policy administration – via the need to align its policy administration system to identify products under the scope of CRS; and
- Underwriting – via the need to modify existing underwriting systems to capture the indicia information for foreign accounts.
IFRS 9

IFRS 9 *Financial Instruments* is effective from 1 January 2018 and replaces IAS 39. There are three parts: classification and measurement; impairment; and hedge accounting. Financial institutions see changes to impairment as the biggest challenge as the incurred loss model is being replaced with a three stage expected credit loss model.

Owing to the increased judgement introduced under IFRS 9, external auditors and regulators are becoming increasingly interested in how financial institutions will deliver a high quality implementation of the new rules. As such, Audit Committees are turning to internal audit functions to provide a level of comfort that key accounting policy interpretations and judgements are appropriate, and that all required changes to systems and processes, including data requirements and internal controls, have been identified and tested so they are appropriate for use in IFRS 9.

**What can Internal Audit do to address this?**

- Make an assessment of progress against IFRS 9 programme milestones and validation of programme governance;
- Carry out a validation of build assumptions and interpretations for accounting policy, models, infrastructure, governance, and disclosures; and
- Conduct periodic reviews of model validation and experienced credit judgement frameworks.
What is the impact on Retail Banking?
Retail banks will see higher and more volatile provisions, a weakening capital position, and a significantly more demanding disclosure regime with the introduction of IFRS 9. Operating margins will be further squeezed due to the need to implement system and process changes across the bank. To offset this, retail banks will be considering strategies to strengthen and protect their revenue streams through product development and realigning risk appetite and business mix.

What is the impact on Capital Markets?
The impact will be very similar to Retail Banking for corporate loan books. Corporate and central banks that issue financial guarantees or debt with large committed undrawn elements will see their impairment stocks rise. Issuers of debt securities will be more closely scrutinised to assess their credit worthiness. Further P&L volatility may be introduced where assets are reclassified to a fair value treatment which may result in changes to product features.

What is the impact on Insurance?
Insurance companies without banking operations may defer implementing IFRS 9 to 2020 to align with the implementation of IFRS 4 Insurance Contracts. However, banks with insurance arms will not be able to adopt this deferral option so they will see an impact on their retail and corporate books as detailed above, and they will need to check to see that their insurance asset portfolios are considered as part of their IFRS 9 programmes.

What is the impact on Investment Management?
Funds will see a similar impact to Capital Markets, however, the scale of impact will depend on the assets within the fund and existing accounting policy treatment. Impact on fund managers will be minimal as assets are typically fair value treated so will be outside the scope of IFRS 9.
IFRS 15 is very detailed in comparison to IAS 18. The principles for revenue recognition under IAS 18 are broad and thus entities would need to use judgment in applying these principles. Under IFRS 15, entities follow a five step model framework in delivering the core principle; an entity will recognise revenue to depict the transfer of promised good or services to customers in an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services.

When identifying and allocating different goods or services within a contract, the lack of specific guidance under IAS 18 resulted in greater room for judgment. Entities may have to amend their current accounting policies, as the new standard requires the revenue from a contract to be allocated to each distinct good or service provided on a relative standalone selling price basis, though a ‘residual’ approach is permitted in limited circumstances.

As a result of these changes, there will be an impact on processes and information systems, and there will be a need to capture increasing amounts of data.

Entities, if not already underway, should perform a business impact assessment of the move to IFRS 15. Key actions include:

- Reassess contracts with customers;
- Assess the impact on financial reporting and key performance indicators;
- Informing key stakeholders and investors;
- Impact on tax;
- Impact on processes, information systems, and data capture;
- Training needs;
- Potential advantages/disadvantages or early adoption;
- Transition approach; and
- Disclosure impact of IFRS 15 ahead of adoption.

What can Internal Audit do to address this?

- During the design and implementation phase, assess the adequacy of resources and required systems and process changes as a result of the move to IFRS 15.
A financial institution that holds US securities on behalf of its clients or engages in transactions that reference US equities must consider its US withholding and tax reporting obligations. One of the ways in which these obligations can be managed is where the firm becomes a Qualified Intermediary (QI) with the US Internal Revenue Service (IRS). This requires the QI to:

- Document its customers and provide for appropriate US withholding and reporting for its customers;
- Submit a certification of compliance to the IRS every three years by the firm’s Responsible Officer (RO); and
- Provide US tax documentation in most cases to mitigate the incidence of US withholding tax on payments received by the QI.

To support the certification of compliance by the RO, there must be a periodic review of the QI internal controls is undertaken that can be completed by Internal Audit or an external advisor.

What can Internal Audit do to address this?
- Consider the design of the controls relevant to QI compliance; and
- Complete the required periodic review of the QI controls, unless an external provider is selected.

What is the impact on Retail Banking, Capital Markets and Insurance?
To the extent that the firm has any business that requires them to collect US source income, or otherwise trades financial instruments referencing US equities, they will need to consider US withholding implications.

What is the impact on Investment Management?
The impact on investment managers will be most relevant where, for example, a wealth manager holds US securities on behalf of its customers, or a fund that they manage enters into financial instruments referencing US equities, to determine whether they will need to consider US withholding implications.
A significant amount of regulatory data is routinely provided by financial institutions to a wide range of users. This includes certain various regulatory ratios and their underlying components, reported in a wide range of end formats such as risk-weighted asset (RWA), Capital Requirements Directive (CRD) IV Financial Reporting (FINREP), CRD IV Common Reporting (COREP) and Stress Testing, sections of the Annual Report (such as the Capital & Risk Management Report), BCBS Pillar 3 reporting and analyst presentations. These regulatory factors fall outside of external audit and Sarbanes-Oxley (SOX), and therefore impact Internal Audit.

This reporting is utilised by a number of different stakeholders, both internal and external. The reporting may influence the decisions made by management, and will also be reviewed by regulators, government bodies, analysts, investors and ratings agencies.

Audit Committees and Senior Managers will need to continue to challenge frameworks over these areas as a result of clearer accountability frameworks.

Enhancing internal control and in particular the organisation's non-reporting frameworks would help to mitigate a range of regulatory reporting risks, including:

- Multiple data sources;
- Data quality – inaccurate or incomplete source data;
- Incomplete reconciliation process and/or unresolved differences;
- Inconsistent design and implementation of control standards;
- Inconsistent output (e.g. between different regulatory returns or other regulatory submissions);
- Unexplained variances; and
- User identified errors.

As a result of this increased regulatory scrutiny, it is expected that enhanced internal control frameworks over all aspects of reporting and disclosure will continue to be a priority area of focus for both Audit Committees and Internal Audit.
What can Internal Audit do to address this?

- Demonstrate adequate coverage of end-to-end data quality and data mapping processes, including controls over the integrity of relevant data storage and transmission;
- Work with management to challenge both design and readiness assessments over data quality, integrity and validation, model governance, review and reporting; and
- Assess appropriate coverage of key topics such as:
  - **COREP and RWA** – important as regulators expect heightened senior management supervision and responsibility for the production and integrity of the firm’s financial information and its regulatory reporting
  - **BCBS Pillar 3** – since a formal board-approved disclosure policy for Pillar 3 information now sets out the internal controls and procedures for disclosure of such information
  - **BCBS 239** – to promote the identification, assessment and management of data quality risks as part of its overall risk management framework.

### What is the impact on Retail Banking and Capital Markets?

COREP, RWA, BCBS Pillar 3 and BCBS 239 (for systemically important institutions) continue to be significant focus areas for Risk and Finance functions across these sectors, including continued enhancements to regulatory reporting processes and control frameworks, and the evidencing of independent review and challenge by functions responsible for oversight. Successful implementation of enhanced Pillar 3 reporting frameworks and BCBS 239 in particular is dependent upon a variety of stakeholders across the organisation, and involves a strategic and cross-functional view of data lineage in particular.

### What is the impact on Insurance?

Further detail in the discussion of SII is addressed in the SII topic. SII is the new capital reporting regime for insurers which went live on 1 January 2016. SII impacts insurers in three main areas which have been called Pillars 1 to 3. Pillar 1 dictates the qualitative and quantitative framework to be used by insurers to calculate their technical provisions and their Solvency Capital Requirement (SCR). This uses either a standard formula supplied by European Insurance and Occupational Pensions Authority (EIOPA) or an internal model developed by the insurance company. Pillar 2 sets out the requirements in relation to the governance and risk management framework that are required to measure the company’s risk against which capital must be held. Pillar 3 sets out the disclosure and reporting requirements, both quantitative and qualitative, for SII reporting to the firm’s regulator. Over the coming years, as SII is embedded, it is expected that insurers will take further strides in how best to refine their capital position and related reporting.
Across EU, Governments are looking to introduce new Corporate Criminal Offences for Failing to Prevent the Facilitation of Tax Evasion. The new offences are aimed at addressing a perceived inability to effectively prosecute businesses whose staff assist in tax evasion.

Penalties for non-compliance are likely to include significant monetary fines and prison terms. Furthermore, action under the new rules would expose an organisation and its senior individuals to significant reputational risk.

The rules will likely require businesses to implement and maintain controls that are reasonably intended to prevent related persons assisting in tax evasion.

The Corporate Criminal Offence follows a broad principles based approach and seeks to build on existing control environments. Organisations are expected to take a proportionate approach that clearly evidences their risk assessments, ongoing monitoring, senior governance of the control environment and culture.

**What can Internal Audit do to address this?**

- Plan for a risk assessment to be performed;
- Plan for a post implementation review of the new controls and processes;
- Carry out a project management audit of the firm's programme to manage risk associated to tax evasion.
What is the impact on Retail Banking?
Retail banks will likely want to incorporate any changes and ongoing monitoring into their existing continual cycle of regulatory change. The banks will need to understand which employees and intermediaries fall within the scope of the requirements which will be a task in itself. Given the scale of retail banks, risk assessments will take careful planning so that the response is proportionate. Additionally, implementing change and evidencing a culture of compliance which is driven from the top down will pose a challenge at an organisational level.

What is the impact on Capital Markets?
The impact on Capital Markets will vary widely depending on the activities. To the extent that businesses provide tailored products for clients, especially where these have any tax efficient selling points, then organisations will need to consider who is advising on this. Similarly, where intermediaries are used to distribute products, this will add a new layer of due diligence.

What is the impact on Insurance?
Life insurers will already be conscious of providing tax advice to clients when providing tax efficient products. The scale of the challenge is likely to be increased by the use of intermediaries that sell the products and the potential additional due diligence that will be required on those persons. The scale of the challenge may be comparable to Retail Banking and insurers should look to perform risk assessments early in order to understand the specific risks for their business.
Contacts
United Kingdom
Financial Services Internal Audit contacts

**Paul Day**
Lead Partner, FS Internal Audit
020 7007 5064
pauday@deloitte.co.uk

**Russell Davis**
Partner, Banking and Capital Markets
020 7007 6755
rdavis@deloitte.co.uk

**Terri Fielding**
Partner, Investment Management and Private Equity
020 7007 8403
tfielding@deloitte.co.uk

**Matthew Cox**
Director, Insurance
020 7303 2239
macox@deloitte.co.uk

**Mike Sobers**
Partner, Technology
020 7007 0483
msobers@deloitte.co.uk

**Jamie Young**
Partner, Regions
0113 292 1256
jayoung@deloitte.co.uk
Building trust | 2017 planning priorities for internal audit in financial services

Luxembourg
Governance, Risk and Compliance

Laurent Berliner
Partner - Governance, Risk & Compliance Leader
EMEA Risk Advisory Leader
+352 451 452 328
lberliner@deloitte.lu

Roland Bastin
Partner - Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu

Stéphane Hurtaud
Partner - Information & Technology Risk
+352 451 454 434
shurtaud@deloitte.lu

Michael JJ Martin
Partner – Forensic, AML & Restructuring
+352 451 452 449
michamartin@deloitte.lu

Marlin Flaunet
Partner – Banking & Securities Leader
+352 451 452 334
mflaunet@deloitte.lu

Eric Collard
Partner - Forensic, AML & Restructuring
+352 451 454 985
ecollard@deloitte.lu

Thierry Flamand
Partner - Insurance & Actuarial Services Insurance Leader
+352 451 454 920
tflamand@deloitte.lu

Jean-Philippe Peters
Partner - Risk & Capital Management
+352 451 452 276
jppeters@deloitte.lu

Simon Ramos
Partner - Regulatory Strategy
+352 451 452 702
sramos@deloitte.lu

Johnny Yip
Partner – Investment Management Leader
+352 451 452 489
jyiplanyan@deloitte.lu

Michael Blaise
Director - Business Risk
+352 451 452 562
mblaise@deloitte.lu

Jérôme Sosnowski
Director - Business Risk
+352 451 451 353
jsosnowski@deloitte.lu
Bertrand Parfait
Director - Business Risk
+352 451 452 940
bparfait@deloitte.lu

Arnaud Barosi
Director - Business Risk
+352 451 452 875
abarosi@deloitte.lu

Arnaud Duchesne
Director - Business Risk
+352 451 454 852
aduchesne@deloitte.lu

Fabien Delante
Director - Business Risk
+352 451 452 848
fdelante@deloitte.lu

Laurent de la Vaissière
Director - Information & Technology Risk
+352 451 452 010
Idelavaissiere@deloitte.lu