The value of assurance in managing risks – Insurance InternalAudit 2016
The value of assurance in managing risks – Insurance Internal Audit 2016

The insurance industry continues to face a wide range of risks and challenges: evolving requirements from UK and EU regulators, the significant pace of innovation and developments in business operating models and, as technology and connectivity increases within these business models, increased cyber and data security risks.

Boards and Audit Committees are seeking to optimise the value of assurance to manage risks real time and for assurance that the insurers’ culture and values are appropriately portrayed in day-to-day business conduct and risk management. Internal Audit (IA) has a key role to play in relation to all of these areas.

2016 will also see a strategic focus across the insurance sector on a range of industry issues, including:

- Management of insurance risk, specifically to: (i) increase the sophistication of models used for pricing, exposure management/ reinsurance placement; and (ii) continually improve claims management processes to reduce loss ratios and claims handling costs.
- De-risking and a focus on the quality of core business.
- Specifically, for personal lines insurers, preparation for Flood Re and improving customer experience.

Aligned to all of these themes is the expectation, as set out in the CIIA Guidance to IA in financial services, for IA to assure on key corporate events and to identify approaches to assuring on the effectiveness of governance, compliance, the risk management framework and culture.

This document provides insights into ways in which IA can provide assurance under five themes:

- Financial crime.
- Ethics, culture and conduct.
- External events and emerging risk management.
- Innovation and business operating models.
- Prudential regulation.
Managing the risk of financial crime continues to provide challenges to insurers:

- managing cyber risks;
- managing other sources of data security risks; and
- financial crime regulatory compliance, notably sanctions screening, anti-money laundering procedures and anti-bribery and corruption. We focus on a particular aspect: preparation for the Fourth Money Laundering Directive.

Recent examples in the press such as TalkTalk demonstrate the public interest and reputational risks that can arise through cyber-attacks. Experts continue to express concern on the scale of the risk and the pressure on companies to address them.

Cyber risk management is more challenging as customer demands become increasingly digital and business models increasingly use digital technology and connectivity.

Digital strategies and change programmes, and managing the risks arising from them, are now a common feature of the agenda for the Board and executive management. Regulatory developments increase the focus further. The requirements of the PRA and FCA, the Data Protection Act as well as the Payment Card Industry Data Security Standard are good examples of existing stringent requirements for insurers to protect confidential customer data. Furthermore, the requirements of EU regulation, anticipated to take effect from the start of 2017, are expected to significantly raise the bar for data protection.

In addition, the growth of cyber insurance policies being sold by insurers has become a key area for many firms to expand their product base. The pricing of cyber policies and product terms/conditions are complex, particularly given the lack of historical data and the exponential growth of cyber-attacks and the resulting class-action legal cases in response to security breaches impacting customers.

IA can provide assurance in many ways and across many areas in relation to cyber risk. Illustrative examples of ways assurance can be provided are set out below:

- Reviewing the risk management framework and strategy for IT and data security, with a particular focus on the frequency of review and refreshment to take account of emerging threats and changes to business models such as the growth in digital channels to market. Such analysis should include a ‘read across’ from externally reported cyber events, asking “Could it happen here and how can we mitigate the risk?”
- Reviewing the preparedness of the Board and senior executives – particularly in respect of cyber security crisis management, which requires a timely response should issues arise.
- Ensuring there is a complete inventory of customer data held, the controls to safeguard this data (such as encryption) and the assurance in place within the business to ensure these controls are effective.
- Providing continuous oversight and challenge to ‘in flight’ digital change programmes, to ensure the design of security controls is adequately reflected within the project and that such controls are effective before any go-live decisions are made.
- Assuring on the adequacy and effectiveness of cyber controls.
- Reviewing the adequacy and effectiveness of security controls at any outsourcers and third parties that hold or process customer data (for example claims handlers, data centres, coverholders).
- Performing a gap analysis of the current ‘as is’ security with best practices such as PCI DSS and ISO 27000, to identify areas where additional controls are required.
- Maturity analysis of the information security management framework – top down from the Board and bottom up practices and policies.
- Assuring on the pricing strategy and product life cycle for cyber insurance policies and products.
Other data security risks

The wide range and increasing sources of business connectivity presents significant security risks: remote working, use of mobile phone and tablet technology for emails and report repository access, portable laptops and USB sticks all present data security risks, in addition to the more holistic, infrastructural information security risks.

Insurers’ policy requirements and processes are always looking to develop mitigation strategies and standard remediation steps should laptops or mobile phones be lost, or to reduce the risks arising should employees’ own technology and devices give rise to security risks or incidents.

IA can assure on how such data risks are mitigated in many ways, for example:

- Reviewing the inventory of remote technologies being deployed by a firm to ensure completeness and review the processes and controls in place to ensure security across them.
- Assessing whether BYOD (Bring Your Own Device) policies are adequately designed (and effectively implemented) for staff to mitigate the risk of using devices (such as iPads) for business purposes.
- Reviewing information security policies to ensure they provide directive controls to reduce the risk, assessing the effectiveness of policy implementation across the insurer.
- Ensuring that appropriate and regular security awareness and training is provided for all staff. Evaluating the effectiveness of such training.
- Ensuring that data loss prevention processes and controls are timely, robust and effective to mitigate any risks arising should a device be lost or stolen.
- Ensuring that reporting processes are appropriate to escalate any breaches and whether appropriate root cause/read across analysis is performed of breaches.


Financial Crime is named in the FCA’s Business Plan and Outlook for 2015/16 as one of the key areas of focus risk. At the same time, from a European perspective, the Fourth Money Laundering Directive (MLD4) introduces and further formalises a number of new requirements.

MLD4 seeks to strengthen the current Anti-Money Laundering (AML) framework in the EU and to address a number of the weaknesses identified by the Financial Action Task Force (FATF). MLD4 introduces stricter rules regarding identifying beneficial owners, Trustees and PEPs. Member States will also be required to maintain a central database regarding the beneficial ownership of all entities incorporated in their jurisdiction.

Firms will have a number of challenges to address with their internal processes, covering their approach towards Simplified Due Diligence (SDD) and ensuring that there is a clear risk assessment in place at numerous stages on the firms AML framework, as there will be greater emphasis on the risk-based approach as a mechanism to identify and lessen the risks associated with money laundering and terrorist financing. MLD4 will become law by 26 June 2017.

IA can assist firms getting ready for the changes in a number of ways, for example:

- A health check assessment of the current systems and controls in place in respect of financial crime within firms.
- Assessing whether a gap analysis has been performed in relation to the impact of MLD4 on the insurer and assessing the adequacy of this gap analysis and any resulting action plans.
- Reviewing and amending your current AML framework in line with the requirements of MLD4, which could involve testing around a firm’s risk assessment processes, client take-on and annual AML planning and reporting.
The FCA has outlined a number of strategic priorities for 2015/16, key to which are:
• developing a strategic market led approach, including ensuring fair and effective competition;
• protecting consumers, with specific focus for the FCA on consumer credit protection;
• individual accountability, focussing on risk culture, the effective implementation of the Senior Insurance Managers Regime and Remuneration practices and the effectiveness of whistleblowing processes; and
• application of new International standards and requirements, specifically EU policies and financial crime.

Boards continue to look for ways to ensure that the tone from the top in relation to risk culture is appropriate and to seek tools to assess whether the desired culture and business conduct is effectively displayed and embedded in day-to-day business life.

We will cover in other sections financial crime and the Senior Insurance Managers Regime. Below we identify three key areas for exploring IA assurance opportunities:
• risk culture;
• whistleblowing processes; and
• business conduct assurance.

Risk culture

Risk management frameworks seek to ensure that risk appetite is clearly defined and that all staff have a clear understanding of how the risk management framework operates. Boards are increasingly looking for ways to ensure that risk culture is appropriately displayed in day-to-day behaviour and aligned to brand values and beliefs. Key to this is ensuring a clear definition of the expected culture for an organisation, clearly articulated values that incorporate risk management expectations and formalised ways to ensure these values are embedded, including means to monitor and assess performance against these values and ensure consistent application across the insurer.

The FCA continues to drive expectations for an appropriate risk culture within insurers, with enforcement actions providing evidence of this. As well as regulatory expectations, business events reported in the press often highlight the reputational and brand damage that can arise where even a perception or allegation of an inappropriate culture exists.

There are numerous approaches to assuring on risk culture and these continue to evolve to best fit regulatory requirements and the needs of the Board. Key to any risk culture assurance is the effective co-ordination between IA, the Board and Risk, as second line of defence, to ensure a consistent understanding of expected culture and the desired measures to assess this.

Amongst the range of ways IA can assure are:
• Providing an assessment on risk culture from the top down. For example, the clarity of ‘tone from the top’ from Board and executive management and the way in which culture is defined, communicated, measured, monitored and reported to the Board.
• Assuring on ‘people’ processes: how recruitment processes assess a candidate’s risk management and business conduct ethics and how the performance management process aligns to appropriate risk management behaviour. For example, the use of psychometric testing in relation to an individual’s likely attitudes and behaviours.
• Reporting on positive and negative indicators of risk management on each audit engagement.
• Assessing whether risk culture is appropriately evidenced through change activity.
Challenge and risk

Risk culture (continued)

- Assessing the effectiveness of the Risk function, as a second line of defence, in facilitating the implementation and embedding of an appropriate risk culture.
- Identifying metrics that can measure culture and implement computer assisted analytical tools to extract data to monitor these metrics on an ongoing basis.
- Assessing the adequacy and effectiveness of processes to assess culture in outsourced and third party arrangements, including culture assessments at the due diligence stage and as part of routine governance and oversight of such activities.

Whistleblowing processes

An effective whistleblowing process is a key tool to ensuring appropriate risk culture and business conduct, through the provision of an effective means to report wrongdoings and concerns for staff at all levels in the organisation.

The FCA included whistleblowing in its strategic priorities for 2015/16 and a joint policy statement from the PRA and FCA was issued on 6 October 2015. Implicit to the requirements is ensuring appropriate whistleblowing processes exist within regulated firms: ensuring processes in place are clearly defined and operating effectively.

Outside of financial service regulation, whistleblowing protection is enshrined in the Public Interest Disclosure Act 1998 – this important piece of legislation protects whistleblowers against reprisals. Public Concern at Work, a whistleblowing charity actively engaged with organisations across different sectors.

Considerations for IA assurance on whistleblowing include assessing whether:
- There is a clearly defined policy which is effectively communicated to all staff.
- Reporting lines for whistleblowing ensure independent assessment of all allegations raised through the process and that the rights and treatment of individuals are appropriately maintained during and after the whistleblowing incident.
- There are robust processes for reporting allegations to senior management and the Board, along with the actions being taken as a result of the whistleblowing incident.
- Branches and international operations are effectively covered by whistleblowing processes and governance.
- There are appropriate mechanisms for whistleblowing at outsourced and third party service providers, particularly where customer outcomes are impacted by this service. Furthermore, whether the insurer has a contractual right to receive reports on whistleblowing allegations made and actions taken as a result.
- Continuous monitoring of whistleblowing incidents can provide a real time challenge of the way in which the incident is handled.
The FCA’s focus on conduct of business continues. Focus areas announced by the FCA in its strategic priorities for 2015/16, specifically for general insurance, included:

- Policy PS15/22, issued on 28 September 2015, on the remedies required to address issues identified in the FCA market study into ‘add-ons’ in 2014, including cross selling across all products sold by an authorised firm and guidance on how add-ons are sold on price comparison websites.
- Consultation on the FCA proposal to introduce a measure of monetary value for general insurance products, for example the publication of claims ratios by product.
- Continuation of the FCA review of commercial claims for SME customers.
- Reporting on the FCA review of controls and effectiveness of delegated authorities, specifically the role of the principal insurer in ensuring adequate and robust systems and controls to effectively select and oversee outsourced representatives (including in relation to their sales practices and provision of post-sales services). We have covered delegated authorities elsewhere in this publication.
- An FCA market study in relation to technology and the use of Big Data (for example web analytics and behavioural data tools such as social media). The study will focus on: (i) potential risks and benefits to consumers and potential barriers to accessing products and services created by Big Data; and (ii) ensuring regulation does not unduly constrain beneficial innovation.

Assurance on business conduct and compliance with FCA regulation is key for IA. To provide this, IA plans should assess the impact of the FCA’s strategic priorities on the insurer and thereby plan to provide assurance on the key topics for the FCA at the most appropriate time, recognising FCA regulation is evolving and also the impact of digital transformation programmes on business conduct at many insurers.

IA can provide assurance in many ways, including:

- Where an in-house Compliance Assurance team performs assurance on conduct risk management separate to IA, IA can perform an effectiveness review on the Compliance Assurance team.
- Assessing the adequacy and effectiveness of emerging risk management and compliance monitoring in respect of the strategic priorities of the FCA as outlined opposite.
- Performing reviews of conduct assurance across several levels:
  - assessing underwriting and claims file review processes to ensure business conduct requirements are addressed in routine first line of defence quality assurance;
  - assessing the adequacy and effectiveness of the customer complaints process; and
  - assessing the effectiveness of conduct risk management, from the definition of risk strategy and appetite, relevance and reliability of MI and governance related to conduct risk.
- Assessing the adequacy of conduct risk consideration within change activity, specifically digital change programmes.
- Assessing the controls and oversight of cross-selling and ‘add-on’ sales management, to ensure there is effective MI and governance to ensure compliance with FCA requirements as these develop through 2016.
- The reliability of claims data by product, in anticipation of any future requirements to report on claims ratio by product.
External events

There is a wide range of external events that impact on insurers. Catastrophe events give rise to claims as part of ‘business as usual’ insurance activity and are managed through routine insurance risk management activity. In this section we explore two other areas:

- macro-economic events, such as the continued low interest rate environment and impact of the slowdown in the Chinese economy; and
- management of emerging risks.

Challenge and risk

Macro-economic trends

Whilst there has been a steady improvement in economic performance in recent years since the banking crisis, interest rates continue to remain low. Many insurers have opted to invest in a range of investment products, to stimulate a higher investment return and hence higher overall profit. While within credit and market risk tolerance limits set by the Board, investment strategies are now more often towards the higher end of risk tolerance than may have been the case several years ago.

The Eurozone continues to face political pressure on the sustainability of its current state, both with Grexit concerns and also the ongoing political debate on the relationship between the UK and EU. Any changes could have a significant impact on the UK economy and the corresponding market and credit risks facing insurers.

There is a risk of a second global economic crash should the Chinese economic downturn impact significantly on worldwide trade and stock markets.

Emerging risk management

Regulators are increasingly focussing on the effectiveness of risk management frameworks, including the way in which the framework provides for the forward looking identification, measurement and mitigation of emerging risks. Managing emerging risks is of paramount importance given the speed with which global events impact on insurers, the pace of change generated by the digital age and the demanding and changing regulatory and legal environment within which insurers operate.

Assurance approach

IA can provide assurance through:

- Assuring on the process for setting credit and market risk appetite statements and reporting on the related tolerance levels and risk indicators.
- Assuring on whether risk monitoring is appropriately forward looking in relation to investment management, to ensure a timely intervention to investment strategy should the need arise.
- Assessing the appropriateness of the frequency with which risk appetite and investment strategy is reviewed by the Board.
- Continuous monitoring on credit and market risk indicators.
- Assessing the adequacy and effectiveness of stress testing/ scenario analyses and emerging risk management in relation to macro-economic trends.
Insurance business models have evolved significantly over the last five years to:
- embrace the digital age;
- explore and exploit growth opportunities globally;
- meet changing consumer needs;
- drive cost efficiencies; and
- optimise the use of specialists and experts.

This has often been through an increased use of outsourcing to provide a wide range of services, either domestically or via offshoring to lower cost environments. Delegated underwriting and claims handling firms are increasingly engaged, either to bring in specialist skills or access new markets globally.

As business models evolve, IA has a significant role in assuring that the business model is robustly controlled. This section examines three areas:
- outsourcing/offshoring;
- delegated underwriting authorities and third party claims administrators; and
- digital change programmes.

### Outsourcing/offshoring

Regulatory expectations are that insurers should have effective oversight and management of outsourced business operations and are responsible for the services provided to the same extent as if they were in-house. Outsourcing takes a wide range of forms: from payroll to IT infrastructure, from customer facing services such as call centre operations to back office functions such as financial control, reconciliation and claims processing.

Outsourcing, particularly using third parties offshore, is increasingly being used to reduce costs, but presents a particular challenge to ensuring effective oversight and management control by the insurer.

Effective management of outsourced business activities requires not only robust contractual arrangements, but also effective day-to-day governance, oversight and control. Ensuring these are in place before outsourced activity starts is paramount to set the right tone with outsourced service providers on the insurers’ expectations.

This is particularly true where regulatory expectations are most prevalent: for retail insurers in the case of outsourced services influencing customer outcomes and business conduct; for other insurance sectors where management responsibilities or control functions may be provided by third parties, such as for protection and indemnity clubs.

### Challenge and risk

IA assurance can take many shapes for outsourced operations:
- Assessing how the insurer’s governance and risk management framework is applied to the outsourcer.
- Assessing the adequacy of outsourcing policies and processes, the completeness of the outsourced service inventory and the effectiveness of the application of the policy to outsourced service providers.
- Assessing the effectiveness of due diligence and decision-making processes in relation to initiating new outsourced activities.
- Assessing the process in place to ensure outsourced contracts are subject to adequate and robust internal review and approval by the insurer, including the appropriateness of clauses to ensure regulatory requirements are fully met by the outsourced service provider.
- Assessing the effectiveness of activities to monitor the performance of outsourced services, including interaction/governance, management information and the use of key performance/key risk indicators.
- Performing visits to the outsourcer to undertake assurance work.
- Determining the extent to which assurance providers and internal audit at the outsourcer can be relied upon, the effectiveness of liaison with these providers, for example, in relation to internal audit plans and obtaining relevant internal audit reports.
- Ensuring appropriate fit and proper assessment processes are in place where outsourcers perform any executive management or control function responsibilities on behalf of the insurer.
Outsourcing/offshoring (continued)

Under Solvency II, there are further rules that need to be complied with for outsourcing. Whilst some of these rules are similar to the existing requirements for insurers under SYSC 13.9, many of the Solvency II rules go into far more detail than in the FCA and PRA handbook and are more onerous, particularly for critical or important outsourced arrangements.

Challenge and risk

Delegated underwriting authorities and third party claims administrators

To optimise the use of specialist underwriters and claims handlers, increase global presence and exploit cost benefits from outsourcing, delegated underwriting and claims authorities continue to be a key feature of the insurance industry.

The FCA has stated the need for such arrangements to be subject to appropriate control and for the insurer to ensure business conduct requirements are met and fair customer outcomes achieved. Furthermore, insurance and reputational risk exposures can be significant where delegated authorities are used.

Increasing the use of delegated authorities worldwide brings with it the need to ensure new authorities in new territories fully understand the expectations of them and the mandate within which they can operate. In such instances geography can increase the challenge in ensuring effective oversight.

IA have a significant role to play to ensure delegated authorities are properly established and controlled once in place. Amongst the ways IA can achieve this are:

- Identifying key data and metrics to measure performance and risk management for outsourced activities and developing computer assisted analytical tools to capture this data for real time analysis by IA.
- Assessing how the outsourcer complies with data protection, confidentiality, termination arrangements and ownership rights, and importantly (under Solvency II) on the quality, seniority and appropriateness of the key persons managing the outsource supplier.

Governance, risk & assurance

Internal audit

Under Solvency II, there are further rules that need to be complied with for outsourcing. Whilst some of these rules are similar to the existing requirements for insurers under SYSC 13.9, many of the Solvency II rules go into far more detail than in the FCA and PRA handbook and are more onerous, particularly for critical or important outsourced arrangements.

- Assessing the effectiveness of due diligence and decision-making processes in relation to initiating new delegated underwriting.
- Assessing the process in place to ensure contracts are subject to adequate and robust internal review and approval by the insurer, specifically in relation to underwriting and/or claims authority limits.
- Assessing the governance and oversight in place over each delegated authority, including assurance activity undertaken by the insurers’ underwriting and claims teams.
- Assessing the effectiveness of escalation and referral processes where underwriting or claims involve significant subjectivity or are towards the top end of delegated authority limits.
- Assessing the timeliness and quality of management information and data obtained from delegated authorities, including MI related to business conduct and customer outcomes.
- Assessing the effectiveness of controls in place to ensure proper management of exposures across delegated authorities where accumulation risks may arise.
- Developing computer assisted analytical tools to capture data, for real time analysis, relating to the business performance, risk management and business conduct of delegated authorities.
Digital change programmes

Most firms are undergoing a digital transformation to some extent and the customer journey is never more complex than today: multiple customer channels, multiple devices for customer contact, a complex spaghetti of integration between legacy and newer ‘customer facing’ systems, integration with social media.

The ability of firms to manage their change programme can be a key differentiator – firms that manage change better than others are able to gain more value from the cost of change compared to their competitors whilst also managing the risk of change effectively. In a regulated environment, the ability to manage change is essential.

IA has a key role to play to assess the effectiveness of the digital change programme across the organisation. Some of the ways IA can achieve this are:

- Assessing the effectiveness of the digital change programme.
- Assessing how aligned the change programme is with broader business strategy.
- Assessing whether the design of the digital change programme clearly incorporates customer needs and ensures FCA conduct requirements will be met.
- Reviewing the systems architecture ‘road map’ – assessing whether changes coming up in the pipeline are consistent with the IT governance and strategic framework.
- Assessing whether IT has the right skills in place to deliver the digital change programme.
- Reviewing the IT systems development lifecycle – whether appropriate risk based controls are in place to manage the risk of systems change.
- Assessing the effectiveness of Board governance and understanding of the digital change programme – Does the Board understand the real risks of change? Does the Board receive appropriate reports on IT?
Prudential regulation

Solvency II (SII) becomes effective from 1 January 2016, although there has been significant effort by insurers over the last few years to ensure readiness for the new regime: ensuring the internal model, risk management framework and reporting are in place to meet the requirements of the three pillars of SII. Once live, the challenge will be to optimise business benefit and the cost of compliance.

In addition to SII, the PRA and FCA have issued the ‘Senior Insurance Manager’s Regime’ (SIMR), stipulating requirements for personal accountability in key Board and control function roles in insurers, which become effective in 2016.

In this section we cover areas for IA focus in 2016 in relation to:
• Solvency II; and
• Governance and SIMR.

Challenge and risk

Once live in 2016, Boards and executive management will look to ensure business benefit and cost of compliance are optimised. Key questions will be:
• Are we getting sufficient benefit from the ORSA process? Are we utilising the internal model sufficiently when making business decisions and strategic plans? Can we run the internal model and ORSA process in a lean, timely and cost efficient way? Can we refine internal model assumptions where appropriate to optimize capital usage?
• Are we challenging ourselves on the effectiveness of systems of governance and risk management?
• Are key control functions aligned and operating within an integrated governance framework (for example reducing duplication of effort, risk oversight and assurance activity where appropriate)?
• Is data quality reliable? Are we optimising the use of data warehousing options? Are spreadsheets adequately controlled?
• Is the ongoing validation process cost efficient and ensuring continuous challenge and insight?

In addition, insurers will continue to ensure systems and processes are in place to meet Pillar 3 reporting requirements, ensuring data reliability and timeliness of preparation to meet the regulatory submission dates.

Assurance approach

From 2016, IA will need to define its role in ongoing internal model validation work, and can provide an independent assessment on whether the validation framework meets SII requirements.

IA can also provide assurance on:
• Whether the ORSA process continues to meet the ‘use test’.
• Whether governance remains effective and adequately evolves as business models and activities evolve.
• The effectiveness of the risk management framework and the risk function.
• The effectiveness of the Compliance function.
• The effectiveness of the Actuarial function, specifically in relation to the key reports due from the Actuarial function (relating to data quality, the underwriting policy and adequacy of reinsurance arrangements) which, for many insurers, will be implemented for the first time in 2016.
• Data governance, specifically where: (i) operating models are evolving, to ensure SII data requirements continue to be met; and (ii) the use of spreadsheets is prevalent to the calculation kernel and Pillar 3 reporting.
• Assurance on Pillar 3 reporting, including the process applied to preparing the various returns, data quality and governance process to review and approve regulatory submissions.
Governance and Senior Insurance Managers’ Regime (SIMR)

The governance requirements of SIMR brings with it specific requirements to ensure the fitness and propriety of Directors, executive management and control function holders. Key requirements are:

- a Statement of Responsibilities for each Senior Insurance Manager, which clearly sets out the areas for which they are personally accountable;
- a Governance Map to illustrate the responsibilities assigned within the firm; and
- pre-approval of all Senior Insurance Managers by the regulator before carrying out the role (individuals who are already approved persons may be ‘grandfathered’ into the new regime).

Developing the Governance Map provides an opportunity for Boards to assess whether systems of governance are clear and aligned: specifically: (i) are individual accountabilities clearly defined and embedded in contracts and job descriptions?; (ii) is Board governance and Committee hierarchy clearly aligned to the SIMR requirements?; (iii) is there a clear articulation of the role of each Committee and is potential duplication in roles and responsibilities identified and avoided?; and (iv) is reporting and escalation from executive management, control function and sub-committees to Board clearly defined, adequate and effective?

In respect of fit and proper requirements, firms will need to have robust procedures for individuals to attain, maintain and demonstrate fitness to perform their role.

High level conduct rules will also apply once the regulation is effective, to almost all staff. Each conduct rule will apply to a person’s conduct in relation to the activities performed in their capacity as an employee or senior manager. Again, firms will need to demonstrate that relevant employees and the firm itself are complying with the requirements.

IA’s role in assessing the adequacy and effectiveness of governance is set out in the CIAA Guidance to IA in financial services, issued in July 2013.

IA can also undertake:

- Internal Board effectiveness reviews, either through facilitated surveys and interviews across the Board, reviewing the clarity and completeness of Committee Terms of Reference, reviewing the extent to which Terms of Reference are adequately and effectively discharged through agendas and meeting packs and the adequacy of minutes kept in relation to meetings.
- A review of the Governance Map to assess: (i) whether regulatory requirements are met and clearly articulated in the governance map; (ii) whether systems of governance are clear and aligned; and (iii) the governance over the Governance Map and key function holders.
- A review of the processes and controls relating to fitness and propriety checks on Board Directors and control function holders, to ensure PRA and FCA regulatory requirements are met.
- An assessment of the framework in place to ensure that the high level conduct rules are appropriately implemented and embedded.
Moore Stephens in the UK

Moore Stephens is the UK’s 9th largest independent accounting and consulting network, comprising over 1,700 partners and staff in 39 locations.

Our objective is simple: to be viewed by clients as the first point-of-contact for all their financial, advisory and compliance needs. We achieve this by providing sensible advice and tailored solutions to help clients achieve their commercial and personal goals.

Clients have access to a range of core and specialist services including audit and tax compliance, business and personal tax, trust and estate planning, wealth management, IT consultancy, governance and risk, business support and outsourcing, corporate finance, restructuring & insolvency and forensic accounting.

Our success stems from our industry focus, which enables us to provide an innovative and personal service to our clients in our niche markets. Specialist sectors include charities & education; culture, entertainment & media; energy, mining & renewables; family offices; financial services; hotels & hospitality; insurance; manufacturing & engineering; member organisations & trade unions; owner managed businesses; professional practices; public sector; real estate & construction; shipping & transport; sport & leisure; and technology.

Moore Stephens globally

Moore Stephens International Limited is a global accountancy and consulting network, headquartered in London.

With fees of US$2.7 billion and offices in 103 countries, you can be confident that we have access to the resources and capabilities to meet your needs. Moore Stephens International independent member firms share common values: integrity, personal service, quality, knowledge and a global view.

By combining local expertise and experience with the breadth of our UK and worldwide networks, clients can be confident that, whatever their requirement, Moore Stephens will provide the right solution to their local, national and international needs.