First line of defence - control frameworks for the insurance sector

Addressing conduct, supervision and related controls
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A focus on conduct and related controls</td>
<td>01</td>
</tr>
<tr>
<td>Building an effective first line control function</td>
<td>03</td>
</tr>
<tr>
<td>Strategy: a unified risk and controls framework</td>
<td>05</td>
</tr>
<tr>
<td>Structure: leveraging practices from the banking sector</td>
<td>06</td>
</tr>
<tr>
<td>Execution: first line of defence monitoring</td>
<td>08</td>
</tr>
<tr>
<td>Benefits: deriving efficiencies from a robust control framework</td>
<td>09</td>
</tr>
<tr>
<td>How can we help?</td>
<td>11</td>
</tr>
<tr>
<td>Case studies</td>
<td>12</td>
</tr>
</tbody>
</table>
Strengthening the first line of defence

The general insurance market is under more intense scrutiny than ever before. The Financial Conduct Authority (FCA) is pursuing its market integrity and conduct agenda more forcefully and taking an increasingly interventionist approach. Digital innovations bring fresh opportunities across the sector, as well as new challenges around managing conduct and operational risk.

There are several conduct related hot topics in the general insurance sector today. Dual pricing is common practice, but it remains controversial. Providing customers with value for money is a challenge, but it can be difficult to judge. Improving transparency, disclosure and the management of conflicts of interest in the wholesale broking market is a priority for the Financial Conduct Authority (FCA), but it requires a long term strategic commitment for firms. New rules on data protection also require firms to assess their current practices, and how they use customers’ and business partners’ data. While these issues affect different areas of the market, they are fundamentally reflecting the same themes – the ability to demonstrate fair and transparent customer outcomes, and uphold market integrity.

With the FCA leading the way, conduct is high on the regulatory agenda in most countries and supervisory expectations continue to grow. In the UK, the extended Senior Managers and Certification Regime (SM&CR) will improve accountability. Both the European Insurance and Occupational Pensions Authority (EIOPA) and the International Association of Insurance Supervisors (IAIS) are taking a greater interest in conduct. The Insurance Distribution Directive (IDD) increases regulatory control across the European insurance sector. Keeping up with change is never easy, but good conduct needs to remain a top priority.

Good conduct is driven from the first line of defence and does not exist in isolation, nor is it the only driver behind a robust first line of defence. Establishing a strong operational grip is the building block on which all business activity depends. An effective first line protects the organisation, helps deliver the strategy and promotes controlled growth. Factoring in key controls around the operational risks associated with digitisation, cost reduction, competitive markets, legacy IT systems, change management or new product lines – to name a few – gives organisations the operational strength to embrace change and create a more responsive market for consumers.

Insurance firms should examine their controls and embed the necessary operational resilience in the first line. This requires a holistic approach, supported by a strong culture, which can rapidly adapt to regulatory change, while keeping customer requirements at the heart of the business. Supported by the second and third lines, the first line of defence should help to promote good conduct and to mitigate operational risk.
Since its inception in 2013, the FCA has continued to raise standards on market conduct. The regulator initially focused on ‘micro’ themes, such as motor legal expenses and add-ons, and made several interventions including banning opt-out selling and introducing prescriptive renewal transparency requirements. More recently, the FCA shifted its focus to broader ‘macro’ themes, addressing senior management accountability through SM&CR, and by conducting market studies to investigate potential concerns in personal and commercial lines.

Regardless of what level of detail the FCA has focused on, its overall goal has never wavered. It has always aimed to improve risk governance and control frameworks. This has been a consistent and recurring topic in thematic reviews, specifically in relation to first line supervision. Consequently, Skilled Person reviews, senior management attestations, remediation and rectification programmes often focus on operational effectiveness and resilience.

The FCA is also actively assessing firms’ culture, business model and strategy. The challenge for insurers and brokers is to achieve a culture that reduces the potential for harm and tries to limit errors in judgment. The firms who are succeeding in this area are applying a systematic, enterprise-wide approach to first line conduct and control frameworks.

The timeline below summarises the FCA’s changing expectations of the insurance market since 2013.

**Recent trends:**
- Oversight of third party distribution, outsourcing and delegated authority
- Board-level awareness of risks around pricing practices, conflicts of interest and ancillary revenue streams
- Cyber resilience, data protection and outdated IT legacy systems
- Awareness of individual accountability under SM&CR
- Oversight and control of activities that are outside the FCA perimeter
- Firms’ response to Brexit

---

**FCA thematic reviews and Market Studies**

**2013**
- **June** Thematic reviews of Motor Legal Expenses Insurance and Mobile Phone Insurance highlight issues in the way both products are designed and sold.
- **October** FCA publishes concerns about the oversight and control of claims activities outsourced to private investigators.

**2014**
- **May** Poor MI and ineffective control frameworks found conflicts of interest. Issues found in a review of household and retail travel claims.
- **July** Price comparison websites criticised for too little product information. FCA confirms the findings of its GI Add-ons Market Study.
- **November** Commercial brokers criticised for poor bribery and corruption controls.

**2015**
- **May** Poor customer experience highlighted in a review of SME claims handling.
- **Review of premium finance raises issues over information provided to retail GI customers.**
- **June** Outsourcing review finds issues in oversight and control of delegated authority arrangements.
- **December** Some improvements found in mobile phone insurance but persistent issues with complaints.

**Regulation - new requirements, rules and guidance specifically impacting the insurance sector**

- **March** Finalised guidance on social media and customer communications.
- **April** Finalised guidance on financial crime systems and controls.
- **July** Finalised guidance on risks to customers from performance management at firms.
- **FCA publishes final rules to improve complaints handling.**
- **September** FCA publishes GI Add-ons rules, including a ban on opt-out selling from 1 April 2016.
“We have previously published details of the difficulties firms found in complying with our renewal transparency rules. We expect firms to have learned lessons from this, and to apply these when approaching regulatory change. Firms should place sufficient focus on systems, controls and resources to meet requirements. They should also ensure that accountability for responding to the changes and requirements is clearly allocated to appropriate individuals.”

IDD: delivering clear, fair outcomes for consumers from the insurance sector published on the FCA website, December 2018

Managing regulatory change effectively
The FCA expects firms to fully implement and embed all legal and regulatory requirements, with robust oversight and effective control. This includes requirements beyond the FCA Handbook, including the General Data Protection Regulation (GDPR), the Equality Act, the Bribery Act and, for in-scope institutions, the UK Corporate Governance Code.

The SM&CR applied to all insurers from December 2018, with distributors following in 2019. Although the Senior Insurance Managers Regime (SIMR) commenced in 2016, the extended SM&CR will still be a ‘game changer’ for the market. Business leaders must demonstrate accountability for the areas and management functions under their responsibility. The certification element of the regime will help to embed accountability and engender a positive conduct-focused culture into first line practices.

Similarly, the IDD presents an opportunity to re-assess their first line oversight, including risk assessment and control frameworks for product governance, delegated authority, TPAs and introducers. This is particularly important where legacy arrangements have typically increased risk exposures, which could lead to poor outcomes for customers.

Historically, the market has taken a reactive approach to FCA findings, and firms have generally enhanced specific control frameworks to address a particular theme. While this may be appropriate for some issues, it is less effective when tackling complex change such as culture or conduct. These changes are too big to manage in a piecemeal fashion and culture needs to be fully embedded across the organisation, from the top down.

July A review finds shortcomings relating to principal firms’ oversight and control of Appointed Representative’s activities
September FCA publishes feedback statement on call for input on Big Data
December Review of intermediaries’ PI cover finds “significant concerns” relating to exclusions

2016 2017 2018 2019

March The Senior Insurance Managers Regime (SIMR) aims to strengthen market integrity and improve accountability
July Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services
August FCA publishes final rules to increase transparency and engagement at renewal, effective 1 April 2017

March Insurance Distribution Directive (IDD) Consultation begins
July Consultation to extend SM&CR to insurers and insurance distributors begins
December UK ILS framework comes into force

June Feedback statement on access to travel Insurance
October FCA statement on firms’ failure to implement renewal transparency rules
November FCA publishes the terms of reference for its Wholesale Insurance Broker Market Study

October FCA launches its market study into Motor and Household Pricing Practices and a wider discussion of pricing fairness in financial services
December Review of household pricing practices and Dear CEO letter

H1 2019 FCA publishes findings of its Wholesale Insurance Broker Market Study, with planned reports on value in distribution chains and pricing practices to follow
January FCA publish Consultation on General Insurance Value Measures
April FCA regulation of Claims Management Companies

First line of defence control framework 02
Building an effective first line control function

Insurers and brokers must have a robust first line of defence, to identify, monitor and mitigate the risk of harm from non-financial risks and exposures.

There are a number of factors to consider when developing, implementing or revising a first line control function. These elements help ensure the control framework is fit for purpose, cost effective and aligned to industry best practice.

How to approach designing a balanced control function:

- The business must drive and own its control framework – they know the business, clients, risks, market impact and employee motivations
- Controls must be effectively designed and embedded to manage key risks and business activities. For example:
  - Firms should consider the commerciality of the business including regions, profit and loss and volumes to analyse potential risks, and misconduct or operational errors
- Front to back process flows in each business can determine areas of priority and identify key control points
- The first line needs to find and fix its own issues rather than rely on the second and third lines
- Shared technology – firms need to consider benefits of using the same technology and data
- Firms need to consider how best to resource first line control functions

Strategy: a unified risk and control framework

- The first line drives the controls agenda and plays an active role in the definition, implementation and improvement of the first line control framework
- A cultural framework is established which drives first line accountability

Structure: an emerging role to support the first line

- The structure of the first line of defence function will be influenced by supervisory hierarchy, jurisdiction and business activities
- The first line risk and control function should not simply be an additional layer of governance. It must enable management to have the necessary degree of support and oversight, while remaining cost effective

Execution: first line of defence monitoring

- Optimise technology and data analytics
- The first line co-ordinates with other control functions for surveillance, supervisory dashboards, benchmarks and conduct
- Separates design from operating effectiveness
- Robust assessment of operational effectiveness

Benefits: deriving efficiencies from a robust control framework

- A controls framework that captures the first line control activities in a structured and transparent form can be leveraged by other areas
- Management of business units which have been established within the first line of defence will streamline costs
- Early identification of control breakdowns and control gaps

Supported by a strong cultural framework embedded across the organisation
First line of defence control framework
Strategy: a unified risk and control framework

Many firms take a siloed approach to risk management across the first and second lines of defence. This can result in inconsistent taxonomies, control frameworks and methodologies, with fragmented IT systems. In addition to duplication in terms of workflow and effort, the output of the risk framework will vary, therefore leading to suboptimal reporting of risks and key controls.

A unified risk and controls framework

A unified approach to risk and control management will address the following four pillars:

**Taxonomy, policy and standards**
- Creating consistent risk and control definitions, descriptions and categorisations
- Establishing a risk universe and controls which can be assigned accordingly
- Devising policies and practical control standards to drive consistent central requirements

**Processes and controls**
- Identifying and documenting end-to-end processes and controls within the first line, aligned to business processes, taxonomy and control standards
- Identifying which controls in the first line function link to those in the second line
- Assigning ownership and accountability for risks, controls and each end-to-end process

**Management information (MI) and governance**
- Appropriate levels of MI to relevant stakeholders, for example, trend analysis may be more beneficial to Senior Management Functions (SMFs), whereas more granular data points may be more relevant to certified staff or risk takers
- Comprehensive escalation procedures
- Reliable, accurate and centralised data sources are used across the first and second line, for example for monitoring and surveillance
- Open controls issues and delayed resolution
- MI items of concern subject to governance forums

**Assessment and issue management**
- Assessing and quantifying residual non financial risks. This is most powerful when informed by regular control testing and a robust incident review framework
- Ensuring assessment is forward looking based on regulatory change, the political landscape and/or new business opportunities
- Creating plans to action identified gaps
- Learning lessons from events that arise

A large number of departments have non-financial risks which must be mitigated. These include key first line functions, operational risk management, compliance, operations and technology.
Structure: leveraging practices from the banking sector

The insurance industry can learn from the banking sector and apply similar techniques to improve controls. Many banks have recently introduced roles which aim to improve synergies across the three lines of defence and take a more holistic approach to financial and non-financial risk management. Some organisations refer to this as ‘Chief Control Officer’ (CCO) or ‘Front Office Risk and Control’ (FORC). In order to establish this function, businesses must have a clear understanding of their existing control environment, how it works across each line and what role the CCO/FORC should have within the structure.

The diagram represents the flow of MI and reporting lines between the three lines of defence and the CCO function. Client and market information will come into the first line, for monitoring and application of first line controls. This same information will come into the second line and be reviewed at the same control points, ideally from the same data source. Compliance will also be checked against the regulatory breach register and evidenced for the regulator. Under SM&CR the accountable executives must have sufficient MI and visibility of the activities being conducted, which is evidence that they are in control of their business activities.

The most observed first line of defence functions fall into one of three broad categories:

**Centralised** – The CCO provides oversight of controls, without direct execution responsibilities. The CCO’s authority and accountability flows through the CCO function.

**Decentralised** (Federated) – The CCO function is focused on controls execution. Authority flows through the business, directly to business heads, COO, Chief Accounting Officer or business manager.

**Hybrid** – Authority flows through the CCO function for some matters and through the business for others. CCOs draw authority from business lines and functions.
Regulation, standards and technology continue to evolve in insurance and across the financial services sector

**Regulation** – the FCA has undertaken a survey of firms across the financial services sector. Their report ‘5 Conduct Questions’, released in April 2018, highlights five key areas of focus, including identification, supporting conduct improvements and oversight and governance. These issues are highly relevant for the insurance sector.

**Industry standards** – insurance firms operate in global markets. Therefore, regulatory expectations need to be supported by industry standards designed by market participants. Market practices should be adopted by firms and, where these standards are developed, the practitioners are incentivised to implement them.

**Technology** – disruption and innovation and the need for operational efficiency is driving insurer and broker strategies in three key areas: data, distribution and customer experience. From a risk, oversight and control perspective, technology solutions can accelerate effective integration between first and second lines, drawing on consistent data sources to establish robust control points across the business.
Controls must be effectively managed across all three lines of defence. At the first line there is an opportunity for earlier identification of issues and intervention. The preventative and detective potential of the first line of defence has increased its importance, and as such, its role has expanded for non-financial risks.

### The role of the senior manager
Some controls are specific to all senior managers across the industry, who must:
- be satisfied that management information provided to them is sufficient
- understand the legal definition of conduct risk and the firm’s exposure
- be able to recognise and articulate warning signs of misconduct
- ensure that people on their reporting lines receive the appropriate training
- develop a consistent data approach and key risk indicators with the compliance team.

---

**Execution: first line of defence monitoring**
**Benefits:** deriving efficiencies from a robust control framework

There are benefits that will be derived from having a robust first line controls framework that is independent from, and works with, both the second and third lines of defence.

<table>
<thead>
<tr>
<th>How can a robust first line of defence be beneficial for the business?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost-effective control framework</strong> 01</td>
</tr>
<tr>
<td>Simplifying and delineating responsibilities from a disjointed controls framework to a holistic approach has delivered significant efficiencies for many financial institutions. Optimising the operating model reduces duplication, streamlines control design and monitoring, and simplifies reporting models.</td>
</tr>
</tbody>
</table>

| **Improved responsiveness** 02                      |
| In the banking sector, a standardised CCO function has allowed many financial institutions to proactively design, prioritise, manage and execute their control frameworks to meet the reporting expectations of senior management and regulators. Additionally, an optimised CCO function can enable greater responsiveness to the rapidly evolving market, operational and conduct risk environment. |

| **Enhanced control governance** 03                      |
| A well-defined governance structure, with exhaustive accountabilities and responsibilities, as well as a clear escalation path, is a key component of an effective control function. Senior managers are held accountable for the effectiveness of the control framework within the business. |

| **Reduced risk of non-financial control breaches** 04                      |
| A dedicated senior manager, accountable for cross-functional supervision of non-financial risks (both operational and conduct-related) within the first line of defence, can be highly effective in building a central framework that reduces operational breaches and identifying lessons learnt, thus enhancing broader risk culture and mitigating the risk of regulatory intervention. |

| **Utilise technology to evolve** 05                      |
| Digital and technology developments play a central role in the evolution of control functions. Senior managers should consider the use of enhanced data analytics, technology solutions and, in many cases, third-party associations, to empower the function through enhanced or automated supervision, management and controls testing to mitigate non-financial risk. |

| **Senior Managers & Certification Regime** 06                      |
| Senior managers have a duty of responsibility to take reasonable steps to prevent regulatory breaches in their area of business. The introduction of a CCO role or equivalent can be a key step in demonstrating that a senior manager has taken those reasonable steps. CCOs not only reinforce the control framework, but also play an important role in ensuring that senior managers understand and meet regulatory accountabilities under SM&CR. CCOs can, in turn, ensure senior managers receive appropriate MI to monitor the activities of their businesses and check that the overall control framework is fit for purpose across all three lines of defence. |
How can we help?

Firms with an effective and robust control framework have undertaken key reviews to assess their current state, and have designed an appropriate framework to improve synergies across the three lines of defence. Our first line of defence health checks can support firms of all sizes to check their current state, identify strategic goals and help businesses to achieve best practice.

Our first line of defence health check

- Supported by effective change management processes
- Practical project management must involve key stakeholders to embed the above framework components

Governance assessment
- Ensuring appropriate roles, responsibilities, hierarchical structure and escalation routes
- Supervisory evaluations, attestation controls
- First and second line delineations

Risk processes and controls
- Risk and control assessments
- Process implementation
- Front to back testing
- Development and implementation of corrective action plans
- Investigations and remediation of control failings
- Attestations and assurance
- Lessons learnt assessments

Technology assessment and monitoring
- Technology assessment for control monitoring and surveillance
- Technology solutions and implementation
- Parameter assessments and change recommendations
- Conducting monitoring and control actions

Culture and SM&CR reviews
- Prescribed responsibilities, organisational structure, responsibility maps and individual accountabilities
- Reviewing Management Information
Case studies

Risk and control framework for third party relationships
An international insurer and re-insurer engaged us to design and implement a new risk and control framework. This was to help it effectively manage its commercial and retail intermediary channels, in line with regulatory requirements.

Our client’s third party portfolio included ‘standard’ and ‘non-standard’ arrangements distributed via complex chains of regulated and unregulated intermediaries. A number of the relationships involved delegated underwriting, claims and complaints authorities.

We established a robust oversight and control environment for our client’s third party relationships, adopting a proportionate and risk-sensitive approach that determined the nature and intensity of controls through detailed technical assessment of inherent regulatory, underwriting and commercial risk.

As a result our client now has a market-leading risk and control environment for distribution that required very limited changes to be IDD-ready.

Insurance sales process mapping governance and control
A large UK insurer engaged us to document its new business sales process for the direct and intermediary channels across its range of products. We produced high quality process maps that detailed existing controls and potential control failure points, as well as insight on potential future regulatory issues. This gave our client a clear and consistent view of its sales process and areas of the highest importance to focus their remedial activity.

Control assurance reviews
We provide over 7,500 days of assurance control activity via outsourced and co-sourced services to clients across the insurance sector. Our assurance work provides objective, expert and risk-focused assurance over all aspects of our clients’ business, to help them reach their immediate and long term goals. By identifying internal control weaknesses and providing pragmatic recommendations to mitigate these, we can help to enhance the internal control state and embed good conduct practices across all three lines of defence.

Senior Managers and Certification Regime
We have extensive experience in assisting global organisations to implement the Senior Managers and Certification Regime. As a result of the regulatory changes, it is essential that senior managers have a granular understanding of the controls they own. We have helped senior managers define the governance structures and terms of reference, provided clarity around role requirements and outlined the challenges with regards to overseas coverage of the regulation.

Risk governance, controls and regulatory change
effectiveness
The FCA challenged our client in relation to its growth programme. We helped the client undertake a far-reaching independent review of the effectiveness and appropriateness of its risk governance and controls. Our recommendations helped our client to meet two key interlinked objectives:
• to demonstrate to the FCA that it had taken the regulator’s concerns seriously
• to ensure its risk governance arrangements would be sufficiently robust and forward-looking to execute its commercial growth strategy safely and stand the test of ongoing UK and international regulatory and stakeholder scrutiny.

Section 166 Reviews - Delegated Authority (DA) Governance and Control
We have undertaken a number of Skilled Person reviews of insurers’ oversight and control of DA arrangements, with a focus on end customer outcomes. These reviews required robust assessment and testing of the design, adequacy and appropriateness of our client’s outsourcing arrangements and the operational effectiveness of the framework in practice.

We gained a deep understanding of the design principles and business standards that defined firms’ control environment. We reviewed the underlying documents, procedures and controls across all stages of the delegated authority lifecycle and undertook extensive sample testing of DA arrangements against a defined maturity model.

Our analytical framework and maturity analysis deliver good outcomes, provide practical recommendations and strengthen firms’ DA governance and control frameworks. Our recommendations integrate well with our clients’ wider product governance and conduct oversight and control standards. Our recommendations are easy to implement and are appropriately prioritised to support sustainable growth.
Contact us

An effective first line control function will have an embedded culture of accountability and sponsor a scalable supervisory framework which supports opportunities for sustainable business growth. We offer best in class advisory and assurance services to support your business in establishing a first line control framework that allows your teams to focus on what they do best.

We are a market-leading specialist in the general insurance sector. Drawing on significant industry experience, we understand the real world challenges you face and the importance of keeping ahead of the regulatory curve. As market dynamics change across the sector, from global commercial re-insurance to retail personal lines, we can support your organisation through proactive horizon scanning and help you to implement sustainable change in line with industry best practice.