Chartered Institute of Internal Auditors

01 March 2018

Conduct risk

Chartered Institute of Internal Auditors

This guide provides an overview of conduct risk and the role of internal audit, focusing on the financial services sector.

Understanding conduct risk

Conduct risk is the term used by financial services firms to describe risks associated to the way organisations, and their staff, relate to customers and the wider financial markets.

The UK Financial Conduct Authority (FCA) has no master definition of conduct risk, however, in its Retail Conduct Risk Outlook 2011, the UK FCA referred to conduct risk as '…the risk that firm behaviour will result in poor outcomes for customers'. Good customer outcomes may be defined as customers getting financial services and products that meet their needs.

In addition the UK FCA has stated that 'a firm's conduct risk profile will be unique to it, and there is no one-size-fits-all framework that can be put in place to assess it.' (Speech by Linda Woodall, Director of Mortgages and Consumer Lending FCA at the Council of Mortgage Lenders (CML) - Mortgage Industry Conference and Exhibition. 6th November 2013).

Firm-specific definitions of conduct risk will need to be reviewed on a regular basis and may need to change in line with lessons learned, changing regulatory expectations as well as changes to the business activities or operating model.

Recent events have demonstrated the importance of maintaining a focus on conduct in both retail and wholesale markets. This has been reinforced through the issuing of rules, guidance, reports or enforcement actions by financial regulators in both the UK & Ireland.

For example, conduct issues relating to Libor, interest rate and Gold benchmarkng have resulted in fines for a number of UK financial services firms. The FCA has also fined firms for breaches of the financial promotions rules, which places even greater emphasis on the need to be clear, fair and not

misleading when issuing financial promotions.

The Central Bank of Ireland has a number of statutory codes of conduct covering topics such as consumer protection, mortgage arrears and business lending. The regulators have also focussed on other conduct risks including compliance with financial sanctions, management of client monies, and affordability for mortgages.

While this guidance focuses on the regulatory requirements for financial services, the implications for conduct risk are much wider than simply providing good customer service. Considering the impact and outcomes of activities on customers, stakeholders and wider society is something that is also relevant for other types of organisations including public sector, private sector and not-for-profit organisations.

Stakeholder expectations

The UK FCA expects regulated firms to be able to focus holistically on conduct risk to ensure financial markets function well. For the FCA this means that:

- Consumers get financial services and products that meet their needs from firms they can trust.
- Markets and financial systems are sound, stable and resilient with transparent pricing information.
- Firms compete effectively, with the interests of their customers and the integrity of markets at the heart of how they run their business.

The FCA uses its Firm Systematic Framework to make forward-looking assessments of firms, and the risks they pose to the FCA's objectives. The firm systematic framework is designed to answer the key question of 'Are the interests of customers and market integrity at the heart of how this firm is run?' The FCA expects firms to focus on conduct risk and to ensure that management of this risk is considered in strategic and operational decision making. A specific assessment may result in a programme of remedial action required of a firm (FCA fact sheet).

Internal audit's role

The primary role of internal audit is to help the board and executive management to protect the assets, reputation and sustainability of the organisation.

It does this by assessing whether all significant risks are identified and appropriately reported by management to the board and executive management; assessing whether they are adequately controlled; and by challenging executive management to improve the effectiveness of governance, risk management and internal controls.

Managing and mitigating conduct risk continues to be one of the highest regulatory priorities for firms and therefore should be integral to internal audit plans, as regulators' attention and resources are firmly centred on the behaviour of firms and how they conduct their business.

The IIA published the Effective internal audit in the financial services sector code in July 2013 (Financial Services Code). In section [B], Scope and priorities of internal audit, Item 6 (e) refers to the 'Risks of poor customer treatment, giving rise to conduct or reputational risk' and states:

Internal audit should evaluate whether the organisation is acting with integrity in its dealings with customers and in its interaction with relevant markets internal audit should evaluate whether business and risk management are adequately designing and controlling products, services and supporting processes in line with customer interests and conduct regulation.

This clearly sets the expectation that internal audit should consider conduct risk in its audit work. The Financial Services Code covers all activities of financial services firms including designing and controlling products, services and supporting processes. The Code builds on the IIA's International Standards for Internal Auditing by providing sector-specific guidance, and re-inforcing the role of internal audit in providing independent assurance over all activities of financial services firms.

The IIA's International Standards do not make specific reference to conduct risk. However, Performance Standard 2120 Risk Management, states that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes, and in determining whether risk management processes are effective consider if 'significant risks are identified and assessed' and 'appropriate risk responses are selected that align risks with the organisation's risk appetite'. Conduct risk and how it is managed being integral to any financial services firm would therefore need to be assessed by internal audit.

Auditing conduct risk

This section sets out the steps internal auditors should consider when conducting a review of conduct risk.

Performing audits of conduct risk – content

Culture, ethics and integrity and how they are controlled through corporate governance are vital elements of conduct risk. There is a clear regulatory expectation that boards need to set and drive appropriate standards when leading the approach to the successful implementation and embedding of conduct risk.

Internal auditors should consider the impact of other audit work over corporate governance and culture and ethics when considering the approach to auditing conduct risks. Guidance on auditing corporate governance and culture is provided by the IIA in separate guidance and will provide a basis for assessing whether the tone at the top and commitment to conduct risk has been established and is working.

Operating in a customer-focused manner is important in addressing conduct risk and it is customer outcomes that may drive the culture and governance of a firm's approach to conduct risk. Any review will need to include providing assurance on the design and effectiveness of controls over conduct risks and the outcomes of these controls. In the Financial Services Code, Section [B] Scope and priorities of internal audit, Item 6 (h), Outcomes of processes states:

Internal audit should evaluate the design and operating effectiveness of the organisation's policies and processes. As part of this evaluation, internal audit should consider whether the outcomes achieved by the implementation of these policies and processes are in line with the objectives, risk appetite and values of the organisation.

In providing assurance over conduct risk, internal audit should consider if the controls in place are adequate and effective to mitigate the risk of poor customer outcomes. It is important that an

organisation should have a good mix of governance and oversight controls as well as controls over specific business processes to ensure that it can demonstrate that corporate risk is being appropriately managed.

Controls should include corporate governance (including 'tone from the top'), accountability across the organisation, culture and ethics, training, management information and reporting, as well as relevant controls over business processes that include conduct as an inherent risk.

The auditor should also consider if the organisation has the right forward-looking view to ensure that emerging risks are identified timely and effective controls are implemented. The UK FCA's 2015-16 Business plan refers to its view of the seven most important forward-looking areas of focus; auditors should consider these and any other emerging risks that may be relevant when considering the risks that impact the organisation:

- Technology may outstrip firms' investment, consumer capabilities and regulatory response
- Poor culture and controls continue to threaten market integrity, including conflicts of interest
- Large back-books may lead firms to act against their existing customers' best interests
- Pensions, retirement income products and distribution methods may deliver poor consumer outcomes
- Poor culture and practice in consumer credit affordability assessments could result in unaffordable debt. This risk may increasingly affect younger people
- The range of issues that need to be considered in unfair contract terms is given sharper focus by developments over the last year in legislation and legal precedents
- The importance of firms' systems and controls in preventing financial crime

Although there may be others, the FCA has indicated that they see the risk of poor customer outcomes in the following areas, all of which fall within the scope of internal audit;

- Complaints management
- Product design
- Mortgage arrears and forebearance
- Financial promotions
- Fees and charges
- Incentive schemes (including performance management)
- Benchmarking
- Corporate Governance
- Remuneration
- Sales Practices

Therefore, as well as specific audits of conduct risk, elements of conduct risk should be considered when scoping the above audit reviews. The FCA provides regular updates on the causes of risk, including conduct risk, and how these risks affect the financial services market and its participants. This is a good starting point for up to date information when planning any audit assignments focusing on conduct risk.

Developing the audit plan

The head of internal audit is responsible for developing a risk-based audit plan based on a documented analysis of risk. Controls to address conduct risks should be in place across the organisation and so it is important that there should be adequate coverage within the annual internal plan.

The approach to auditing conduct risk in an organisation must be proportionate to the size, scale, complexity and regulatory environment in which it is operating.

In preparing the audit plan, the head of internal audit may wish to consider the following approaches:

1. A specific audit of the conduct risk framework covering oversight, governance, risk appetite, MI and reporting, etc, that looks at the firm's holistic approach to conduct risk, and consider how conduct risk and focus on customer outcomes are considered in strategic decisions. This may include the activities of the first and second line of defence.

2. As previously mentioned, incorporating conduct risk into other audit assignments such as those that have touch points with customers or implications for market risk. Conduct risk applies across all part of an organisation from product development, marketing and sales through to after sales servicing including the management of arrears and overdrafts. Internal auditors should consider the implications of conduct risk in each audit and incorporate an assessment of the management of this risk, where appropriate

In determining the audit plan, consideration should be given to the expectations of key stakeholders, such as the audit committee and regulators. These stakeholders will expect internal audit to provide an assessment of specific conduct risks and an overall opinion on the management of conduct risk within the organisation, both current and forward-looking. The head of audit should ensure that the audits in the plan will, when completed, provide internal audit with sufficient evidence to meet these reporting expectations.

Research and gather background information

In planning any audit review of conduct risk there will be a need to identify the specific conduct risks that are relevant to the organisation. If the organisation has not yet identified its own view of the conduct risk to which it is exposed, internal audit will need to identify these. A good starting point will be to refer to regulatory requirements in the UK FCA's Handbook such as the business standards (including the conduct sourcebooks) which provide the detailed requirements relating to firms' day-to-day business; Redress which includes the processes for handling complaints and compensation; and specialist sourcebooks which cover the requirements applying to individual business sectors.

In order to determine any additional audit activity that is not already included in the audit plan, internal audit may consider mapping the conduct risks in the handbook to the audit universe. Any gaps in audit coverage can easily be identified and additional / expanded scope audits included, as required.

Discussion with other stakeholders both within the organisation and externally, to understand their respective concerns and priorities, may help to formulate the plan and approach.

In addition, the internal auditor should obtain and review business information and data (e.g. operational losses/near misses, volume /type of customer complaints, policy / risk appetite breaches) which will help the internal auditor to understand the actual / potential impact of conduct risk on the organisation.

Other assurance providers and the need for coordination

The Institute's International Standards support the idea of effective coordination among assurance

providers. Performance Standard 2050 - Coordination, states: 'The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimise duplication of efforts'.

This is addressed in the guidance published by the IIA entitled Coordination of assurance services . Where appropriate, there should be discussion and co-ordination between internal audit and other assurance providers, to avoid duplication of effort, where possible.

Organisations in financial services should also refer to section [D] of the Financial Services Code, Interaction with risk management, compliance and finance, which makes clear that in no circumstances should internal audit rely exclusively on the work of risk management, compliance or finance and that it should exercise informed judgement as to when to place reliance on their work. To the extent that internal audit places reliance on the work of these functions, that should only be after a thorough evaluation of the effectiveness of that function in relation to the area under review.

Skills and experience required

The skills, experience and knowledge required by the auditor(s) who will be completing the review should be identified. The auditor(s) will need to have an appropriate level of understanding of the organisation and its business, its strategy and objectives, risk appetite and values. This will help the auditor(s) to have a good basis from which to identify the conduct risks faced by the organisation. The auditor(s) will need have an understanding of both regulations and regulatory expectations relating to conduct risk and be able to use this knowledge effectively when assessing the controls in place around conduct risk.

Where the internal audit function does not have the specific skills or experience, consideration should be given to using co-sourcing arrangements to complete the audit (or to fully outsource the completion of the audit).

The internal audit function should be able to evidence that the audit work has been completed by resources with the appropriate skills and experience.

Conducting an audit of conduct risk

The first step is to establish whether management has defined what “success and good” looks like in terms of conduct risk for the organisation and whether it has identified the conduct risks which are relevant to the organisation. Obtaining a copy of the organisation’s objectives and risk appetite is a good starting point in assessing the risks that the organisation may face relating to conduct risk. Understanding the values of the organisation (where defined) will also help the auditor to assess the potential impact of conduct risks faced by the organisation.

Next, the auditor should confirm if management has adequately identified and assessed the risks related to conduct risk and whether management considers that they have adequate controls in place to manage them within a defined risk appetite and stance on conduct risk and culture. All firms need to be able to measure and report on the qualitative as well as any quantitative elements making up the diverse concept of conduct risk, the auditor should confirm if this is place and operating effectively.

Once the auditor has determined the scope of the audit, and the risks which will be assessed, these should be discussed and agreed with senior management prior to commencing the audit review.

For internal audit reviews that have touch points with customers, in addition to assessing the

adequacy and effectiveness of controls, the internal auditor should identify the expected customer outcome(s) and assess whether or not the outcome has been achieved. Consideration should be given to the use of one to interviews, workshops and surveys in determining whether outcomes have been achieved, gaining an insight into the prevailing around treating customers fairly and understanding the root cause of issues that have arisen.

Internal audit should report any failings identified during the audit review and be prepared to provide advice to management in taking remedial actions.

Where internal audit identifies instances of suspected or actual breaches of regulations or best practice guidance, this should be brought to the attention of the board, the audit committee and senior management as soon as possible.

Examples of conduct risk

As explained, an organisation's conduct risks will be unique to it and there is no 'one size fits all' framework. Consideration needs to be given to changes that are required to address lessons-learned, changing regulatory expectations as well as changes to the organisation's activities or operating model.

With this in mind, the example below which refers to risks and controls for complaint handing should be considered as an example only. Auditors will need to identify and assess the conduct risks specific to their organisation.

1. Customer complaints are not resolved timely or appropriately adversely impacting the reputation of the organisation and increasing regulatory risk.

2. The root causes of customer complaints are not identified and actions are not taken to prevent the complaint from reoccurring leading to increased reputational and regulatory risk.

3. Redress is not offered to non-complainants (who are impacted by the same issue as a customer who complains) leading to increased reputational risk.