



Financial Conduct Authority

Internal Audit final report

A review of risk management and the implementation of the first and second lines of defence.

Findings identified	
Major	3
Moderate	0
Minor	0

7 January 2014

1 Executive Summary

1.1 Summary and opinion for Audit Committee

Context

In December 2012, ExCo decided that the FCA would implement a 'three lines of defence' model for risk management. It was agreed that there would be a first line of defence that managed and owned its own risks and controls and a second line that would provide an independent view of risk, assurance on risk management and a risk framework with common standards. A move to this model required cultural as well as procedural change and a repositioning of the roles of some staff working in the first and second lines of defence.

In March 2013, the Policy, Risk and Research (PRR) Division underwent a restructure. This restructure included substantial changes to the Risk and Strategy Department. We recognise that these changes have created challenges and uncertainty for staff within the Risk Function.

In March 2013, the components of a 'risk architecture' were taken to ExCo and broadly agreed. Work therefore began on developing risk management tools and processes, including agreeing the split between 1st and 2nd Line responsibilities. In July 2013, on the basis of this work, ExCo agreed to 'switch on' the 1st and 2nd Lines. In July 2013, ExCo also decided that a 'working group' would be created to assist the development of the first line of defence. Initial ExCo expectations were that attestations from the first line would be complete by January 2014 and that the Risk Function would perform review work of the effectiveness of the first line in October 2013 and again in January 2014. However, at a July ExCo, it was recognised that the timeline for first line attestations would need to be revisited. Subsequently, the October Risk review was cancelled due to the timing clash with this Internal Audit review and the January review was postponed to March 2014. At the time of our review, work remained on-going in the business to identify and assess the first line controls.

Review Findings

A significant amount of work has taken place since the end of 2012, examples of which are set out below:

- Although the CRO role required further development, we saw the CRO providing a more prominent independent view of risk.
- The first line working group were engaged in understanding their risks, controls and how they monitor control effectiveness.
- There was progress and continued focus on the development of risk management tools and processes such as divisional risk appetite statements.
- The Risk Committee reporting had been enhanced.

Despite the progress highlighted above, increased momentum is now required to finish implementation and embed. In our view, renewed focus and communication is required to capitalise on the work already undertaken, by clarifying what type of risk model the FCA wants, and providing more structure around its implementation. We agreed three Major rated findings and actions with management for the following significant issues:

- Staff we spoke to did not have a clear understanding of what type of risk management approach ExCo wanted for the FCA, the resources it was willing to commit, or how the various risk management tools and processes interrelated.
- The roles and responsibilities of the first and second lines were not widely understood and needed to be considered and clarified, in particular, the empowerment of the Risk Function to oversee the implementation of the overall risk management approach and to provide advice and guidance to the first line without compromising its ability to take an independent view.
- The lack of change management discipline applied to the overall implementation of the lines of defence model. There was no clear ownership of the implementation, nor were there clear deliverables, success measures, or a plan.

We acknowledge that many of the issues above have been raised or questioned by the Risk Function and key stakeholders within the last year. However, implementation of the lines of

defence has not been delivered in the timescales expected in spite of significant resources being applied. Without a plan, clear deliverables or success measures, it is not clear how far along the journey the FCA is in delivering the risk management approach that ExCo wants.

Confirmation work

During this review we also considered the progress made against the recommended outcomes from the 2012 Internal Audit review of 'Internal and External risk management in the Conduct Business Unit' (of the FSA). Based on our fieldwork during this 2013 review we found the outcomes arising from three of the findings of the 2012 review had been achieved. These related to the ownership of an enterprise-wide view of risk, the development of risk committee responsibilities (such as DSRC) and reporting to the Audit and Risk Committees.

The outcomes arising from the remaining three 2012 findings are closely connected to the findings and issues raised in our 2013 review, and as such we have judged that the recommended outcomes have not been achieved. These 2012 review findings related to the design and operation of the lines of defence, development of a risk framework for the FCA and identification and monitoring of key business processes and controls. The new recommended outcomes and actions addressing the three findings of the 2013 review will also address the outstanding outcomes from the 2012 review.

Active monitoring

Given the ongoing nature of the work to implement the first and second lines of defence, we will actively monitor the actions included in this report, including reviewing key papers being presented to committees.

1.2 Overall management comments

This review has come at a good time, a year after the original report highlighted a series of important questions, most notably whether the FCA wanted to move to having a three lines of defence model (3LOD) and a chief risk officer. Having decided in favour of both, a great deal of work has gone in across the FCA to implement 3LOD and build the CRO role, and we are pleased the review recognises the progress made on these.

The nature of the review's findings (around the risk framework, roles of 1st and 2nd lines and change management disciplines) highlights in part the scale of the shift we are making - about culture and communication as well as roles and processes. Reflecting this, for the proposed management actions to succeed will require both the active support of ExCo members and effective work between 1st and 2nd lines.

That said, I believe many of the building blocks needed to achieve the review outcomes have already been agreed by ExCo or have been recognised through our work with the 1LOD Working Group. We will bring these together and use them, alongside recognised standards of good practice in the public and private sector (including from the PCBS report) to set out, in a single document, the FCA's vision and framework for risk management, including the clear roles and responsibilities of 1st and 2nd lines. Once approved by ExCo, we will then plan and oversee its implementation