Financial Conduct Authority

Internal Audit report

The FCA's incident response and crisis management capability

Findings identified	
Major	**2**
Moderate	**1**
Minor	**0**

24 October 2014

1 Executive Summary

1.1 Summary and opinion for Audit Committee

Background

Our audit assessed the FCA's current incident response and crisis management capability and evaluated the extent to which the organisation can respond effectively to incidents and crises.

We evaluated the FCA's current control framework taking into consideration relevant principles and good practices from the May 2014 British Standard on Crisis Management (BS 11200:2014). We also considered the flexibility and responsiveness of the FCA's approach to responding to different incident and crisis scenarios.

Conclusion

We observe that the FCA has a number of independent processes designed to enable the organisation to respond to incidents which could occur. Some of these processes are well established e.g. the Impact Management Framework and Authorities' Response Framework. (Note: the FCA only owns the first three frameworks below). The main processes are the:

1. **Impact Management Framework (IMF)** which is owned by the Operations Division and deals primarily with the response to operational incidents such as those affecting the building or staff wellbeing;
2. **Issue Response Team (IRT)** structure created by the Communications & International Division to address 'key issues' that have long-term implications for the organisation;
3. **Interruption Response Framework (IRF)** which is co-ordinated by the Resilience team in the Policy, Risk & Research (PR&R) Division and details the FCA's response to firm interruptions;
4. **Authorities' Response Framework (ARF)** which covers the co-ordinated response required by the FCA, Bank of England (BoE) and HM Treasury (HMT) to an event that results in major disruption to the financial sector and/or to the Authorities (i.e. FCA, BoE and HMT); and
5. **Finance Gold** process to respond to major emergencies. This is a subset of the central government's Cabinet Office Briefing Room (COBR) support and response framework.

We identified some areas of good practice in these processes which we consider could be more widely applied. These include:

1. the Impact Management Team (IMT) structure as the ultimate point of escalation in the IMF; and
2. requirements in the ARF for external stakeholder engagement by the FCA, Bank of England and HM Treasury.

The FSA's *Incident Management Framework* covered all types of incidents from operational to market incidents. This framework distinguished between incidents and crises and set out the functions responsible for responding to an incident or a crisis and processes to be used and recovery times for various processes based on the priority ranking of these processes. The Crisis Management Team was supported by several teams including Financial Stability, Communications and Legal Counsel, with clearly set out horizontal and vertical coordination between the teams.

We acknowledge that some elements of the FSA framework could not be carried over to the FCA as responsibilities such Financial Stability moved across to the Prudential Regulatory Authority (PRA) at legal cut-over. However, the FSA framework would have provided the FCA with a sound basis on which to develop its approach to incident response and crisis management.

Recent activity

During the course of fieldwork, the IMF framework, including the IMT structure, was tested for a scenario with operational and regulatory components. We welcome this exercise and support the work of management in utilising the results of this test and planned future tests to inform the development of the FCA's capability to respond to incidents.

Accountability, Policy and Framework

The work undertaken by the FCA to date, in incident response and crisis management, can be enhanced in some areas to drive greater consistency and build organisational capability. Specifically, the FCA response processes are largely independent of each other, not mutually supportive and lack consistency of approach. This is largely because they have been created independently without an overall owner for incident response and crisis management, an Incident Response Policy, standards, and overall common framework.

Governance and decision making

Although it is clear that staff have adopted a best endeavours approach to develop response processes, the lack of overall governance is also reflected in inconsistent approaches to evaluating incidents. It is unclear, for example, what constitutes business as usual incidents and what should be escalated as a crisis. The decision to escalate is left largely to the judgement of individuals and, while this is expected to some extent, there is an absence of broad guidance to support these decisions; the provision of some guidance is common practice in most response frameworks. The governance arrangements for FCA owned documents are unclear and other than in the IMF process, documentation lacks defined owners and version control. In addition, the authority and current status of documentation could not be confirmed in most cases.

Delegated authority

The operational incident management process (IMF) defines the decision making authority and process; senior teams are identified with authority to act on behalf of the FCA. Other internal response processes do not have such clarity although these processes assumed that ExCo would be called to manage crises. The delegated authority of some members of the ExCo to act on behalf of the FCA was not clear in all cases.

Building capability

While some limited training has occurred in recent weeks and there is the intent to develop an exercising programme, there is currently no evidence of progressive training in response processes that could be considered sufficient for the purposes of the organisation. In addition, some significant aspects of the FCA's responsibilities are not covered in the current processes, in particular the response to a fast-moving regulatory issue which should be addressed.

We raise three findings relating to the organisation's incident response and crisis management capability. These cover the need to:

1. Establish clear governance arrangements including assigning ownership of the response approach, framework and agreeing delegated authority for decision-making.
2. Define a common response framework within a Policy with guiding principles which sets out a generic FCA process to be followed to drive a consistent approach and coordinated action across the organisation during response. This should as a minimum encompass the Operations, Communications & International, PR&R, Supervision and Markets Divisions.
3. Strengthen the organisation's capability to respond to incidents by increasing staff awareness and capability, including scenario exercising to practise decision making under pressure.

The implementation of the agreed management actions relating to these findings should result in a clearer and more consistent approach to how incidents are identified and responded to by the organisation.

We would like to acknowledge the co-operation and positive engagement shown by stakeholders involved in this review.

1.2 Overall management comments

Thank you for the internal audit report on the topic of the FCA's incident response and crisis management capability. We accept the findings as described.

It is evident that as an organisation, we run a number of very different risks whilst trying to ensure that we meet our statutory objectives. Risks and issues can crystallise from a number of sources and areas (e.g. people, firms, markets etc), which are difficult to predict and often unexpected. In addition, these risks and issues can migrate into 'incidents' or a 'crisis' within a rapid time frame. As such, it is imperative for the organisation that our incident response and crisis management processes work well and are embedded within all the relevant areas.

As such, we take seriously any findings in relation to this area.

We acknowledge that the organisation has a number of independent processes, designed to enable the organisation to respond to incidents which could potentially occur (both operational and regulatory). Due to the breadth and potential complexity of issues that we may face, various frameworks have emerged over time to meet the requisite needs and requirements of the FCA, often for very specific issues/events (e.g. the Authorities' Response Framework (ARF)).

We accept that the overall structure in place does not provide sufficient clarity within the organisation, and would benefit from the implementation of a single consistent framework, with clear lines of delegated authority and which is embedded within the organisation.

We will enhance the current frameworks structure to provide a single framework to meet your 'recommended outcomes'. We intend to continue utilising the principles of ensuring that any framework we implement is complementary to existing frameworks, and is simple, clear and easy to invoke. Additionally, as suggested above, due to the complexity and pace of issues faced, we will provide clear policies and processes for staff for a variety of scenarios, including the uncontrolled release of price sensitive information. However, in practice we are reliant on the judgment of our staff to act appropriately in specific circumstances, so we cannot be overly prescriptive. We must continue to trust our staff to be able to exercise their judgement in dealing with issues and allow them to be empowered to make decisions. We agree that we will make regular review of, and test the framework, and agree that lessons from exercising against various scenarios will allow us to further improve the framework.

We note that with the majority of your findings, there exist a number of interdependencies, and we will undertake careful consideration and analysis of what actions to undertake to remediate the issues you have identified.

Management agrees with the findings of this report and some of the actions to address them are already underway. Where we can undertake any additional actions in an effective manner within a short timeframe, we will endeavour to do so.

On the more substantial actions, where relevant, we will request decisions from the appropriate executive committees, and allow for appropriate consideration of the correct remedial actions that flow from these decisions.

Please refer to the detailed actions below for the detail in each area.

1.3 Schedule of findings

Ref	Findings	Rating
1	Existing governance arrangements over the organisation's approach to incident response and crisis management are inadequate.	**Major**
2	The FCA does not have a single overarching framework in place to support staff in implementing effective responses to incidents and potential crisis situations.	**Major**
3	Further work is required to improve the capability of FCA staff members to implement appropriate and timely responses to incidents and crises.	**Moderate**

2 Detailed findings

1	**Existing governance arrangements over the organisation's approach to incident response and crisis management are inadequate.**	**Major**

The governance arrangements over the FCA's incident response and crisis management approach are not clear. As a result, it is not possible to establish a consistent view on:

- who is accountable for the FCA's approach to incident response and crisis management;
- who has approved delegated authority to act on behalf of the FCA in the event of an incident or crisis; and
- what the roles and responsibilities of particular FCA staff members are during an incident or crisis.

A lack of adequate governance may result in inappropriate actions and decisions being delayed while authority is sought for making decisions or actions being taken on behalf of the organisation by individuals without the required authority to act.

Accountability

There is no overall owner for incident response and crisis management. This has resulted in a series of best endeavours, but inconsistent efforts, by different areas of the FCA to develop incident response or crisis management plans and processes.

The Impact Management Framework (IMF) for responding to operational incidents and maintaining business continuity is the most evolved process in place and ownership of the IMF is defined. For all other response processes, the respective Director is assumed to be the owner of a particular process. This, however, is not clearly set out or communicated. In addition, there are many documents relating to various processes where it is not clear how these documents interrelate or who owns these documents and is responsible for updating these documents.

Delegated authority, roles and responsibilities

The Impact Management Team (IMT) is the designated decision-making team for operational incidents and is made up largely of ExCo members. The decision-making body for other types of incidents is not defined but generally assumed to be ExCo members. Whilst the members of the IMT and supporting teams are specified in the IMF documentation, the roles, responsibilities and delegated authorities of these members are not detailed. A number of the individuals from the IMT we interviewed agreed that further clarity over the roles, responsibilities and delegated authorities would be beneficial.

Decision-making processes

In addition to the IMF, the FCA operates an Interruption Response Framework (IRF) which covers the FCA's response to firm interruptions, such as system outages. The decision-making processes for the IMF and IRF are defined in the form of flowcharts. These processes require staff to make decisions although these decision makers are not identified. In addition, some stakeholders from the IMT we interviewed were not clear about who would make decisions in the absence of a Director.

An absence of clearly appointed decision makers with delegated authority to act can result in inappropriate decisions by unauthorised people or actions being delayed while authority is sought.

Recommended outcomes		**Management actions, owner and date**	
1.1	Accountability for responses to all types of incident is clarified and an Executive is appointed to own the overall incident response and crisis management approach.	**1.1a**	Action: At present responsibility for the IMF is delegated to the COO. As further scenarios are developed and the overall framework is confirmed ExCo will confirm overall ownership of the framework. Owner & Dept: CEO Date: 28 November 2014

1.2	A common response framework that drives consistency of response is in place and an incident/ crisis decision-making body is appointed and authorised to make decisions on behalf of the organisation.	**1.2a**	Action: An overarching structure which clarifies how the components of the FCA response come together in response to different types of scenarios will be developed and published across the organisation. As part of this work, the structure will make clear the accountability for responses to all types of incidents. Owner & Dept: Head of Department, Operations Services and Procurement, Finance and Operations Date: 31 December 2014
1.3	Delegated authorities and decision-making powers in incident and crisis situations are clearly set out and communicated. These include arrangements in the absence of the Chief Executive and appointment of deputies as appropriate.	**1.3a**	Action: An appendix to the overarching structure will be included to clarify authority to act/decision making powers within the overall framework (e.g. the minimum requirements for a decision to be made in a particular event/issue). This appendix will ensure that powers to act are clear, and ensure that the framework is flexible and consistent enough to meet the needs of the FCA e.g. escalations in one area of the framework may require a wider response which is escalated to a different body. In preparing this appendix existing Terms of References (for key executive committees), Board delegations to committees and individuals, and emergency decision making arrangements, will be revisited and re-communicated to those involved. Owner & Dept: Head of Department, Operations Services and Procurement, Finance and Operations Date: 31 December 2014
1.4	The ownership, review and approval requirements of incident response and crisis management documents should be clearly specified and observed. The interrelationships and purpose of documents are clarified.	**1.4a**	Action: As part of the overarching documentation, ownership of the relevant documentation will be assigned (to areas/individuals) to ensure that the framework documents remain up to date, embedded and linkages are made clear. Additionally, a review cycle will be set-out (specifying the frequency of document reviews). Owner & Dept: Head of Department, Operations Services and Procurement, Finance and Operations Date: 31 December 2014

2	**The FCA does not have a single overarching framework in place to support staff in implementing effective responses to incidents and potential crisis situations.**	**Major**

The FCA has a number of disconnected siloed incident response processes with no common framework for escalating incidents to senior decision makers. How the organisation assesses and responds to incidents and crises is inconsistent between divisions and how and when these are escalated is unclear to us. Lack of a directing policy and supporting standards has resulted in a best endeavours approach by staff in formulating an approach to managing an incident or crisis. Consequently, there is no common process to inform and consult stakeholders across the organisation, including ExCo members. This leaves the FCA vulnerable to reputation risk, at a minimum, in the event that the severity of an incident is incorrectly assessed and handled. The existing processes include:

- the **Impact Management Framework (IMF)** which is owned by the Operations Division and deals primarily with the response to operational incidents such as those affecting the building or staff wellbeing;
- the **Issue Response Team (IRT)** structure created by the Communications & International Division designed to address 'key issues' that have long-term implications for the organisation;
- the **Interruption Response Framework (IRF)** which is co-ordinated by the Resilience team in the Policy, Risk & Research (PR&R) Division and details the FCA's response to firm interruptions;
- the **Authorities' Response Framework (ARF)** which covers the co-ordinated response required by the FCA, Bank of England (BoE) and HM Treasury (HMT) to an event that results in major disruption to the financial sector and/or to the Authorities (i.e. FCA, BoE and HMT); and
- the **Finance Gold** process to respond to major emergencies. This is a subset of the central government's Cabinet Office Briefing Room (COBR) support and response framework.

The ARF and Finance Gold are not frameworks owned by the FCA.

While there is much that is useful in the separate approaches, these processes do not represent a single overarching framework covering the identification and response to incidents and potential crises. The FSA's *Incident Management Framework* covered all types of incidents to from operational to market incidents. This framework distinguished between incidents and crises and set out the functions responsible for responding to an incident or a crisis and processes to be used and recovery times for various processes based on the priority ranking of these processes. The Crisis Management Team was supported by several teams including Financial Stability, Communications and Legal Counsel, with clearly set out horizontal and vertical coordination between the teams.

We acknowledge that some elements of the FSA framework could not be carried over to the FCA as responsibilities such Financial Stability moved across to the Prudential Regulatory Authority (PRA) at legal cut-over. However, the FSA framework would have provided the FCA with a sound basis on which to develop its approach to incident response and crisis management.

The existing arrangements could be improved by introducing a framework that draws together different types of incidents from operational to market incidents. The FCA's existing processes do not address a number of points identified as good practice by the British Standard on Crisis Management (BS 11200:2014). The following points should be considered:

- **Policy and minimum standards** – incident response is not covered in the Business Continuity Policy and there are no FCA minimum standards to be applied in incident response. This lack of standards directly contributes to the lack of consistency in response to potential incidents.
- **Escalation criteria** –escalation triggers and paths exist in Divisions and in relation to certain incidents, such as operational incidents. However, these are not consistently applied across the organisation and only the IMF has in place call cascade details i.e. - call information including mobile and home numbers or clearly defined timelines in place.

Escalation triggers and paths provide a useful guide to management and help to mitigate the risk of delays in response as they provide clarity over the transition from "business as usual" to crisis.

- **Tools and templates** – there are few tools and templates to support staff in the implementation of an incident response. This may result in the risk that staff may be uncertain as to what is expected of them and their resulting response may be either slow or inappropriate.
- **Testing requirements** – an operational test was recently conducted but there is no progressive programme of testing and training to ensure staff know what to do and that processes are fit for purpose. Without regular testing, it is not clear how management can gain assurance that the planned approach to respond to incidents is adequate.
- **Co-ordination of stakeholders** – the existing processes do not specify how co-ordination should be managed between different teams involved in incident response. With the exception of the ARF framework, the other existing processes do not set out how and when external stakeholders should be engaged, or show the horizontal coordination required between teams in the event of an incident, or show the engagement of teams such as General Counsel Division where needed. This could result in a disjointed organisational response to incidents.
- **Crisis communications** – although the Director of Communications & International Division was able to articulate how a communications response would be implemented in the event of an incident or crisis, this is not documented. There is the risk that in this individual's absence, communication responses implemented could be ineffective or poorly co-ordinated. Crisis communications should be specifically drawn up as a separate process defining roles, including deputies, and responsibilities.
- **Learning from 'near misses' –** there have been a number of 'near misses' where the IMT has not been invoked but has been informed. However, these 'near misses' have not been assessed to identify remediation or actions for improvement.
- **Post-incident reviews** – there are no common arrangements or requirements for post-incident reviews to identify lessons learned. These post-incident reviews would enable the organisation to identify and address weaknesses in existing processes.

In aggregate, these identified gaps represent significant weaknesses in the FCA's existing arrangements to promptly and effectively respond to incidents and crises which could result in reputational damage to the organisation if a response is handled poorly.

Recommended outcomes		**Management actions, owner and date**	
2.1	A governing policy and supporting standards for incident response and crisis management are in place and enforced. This should include a common framework for the identification, assessment, escalation and response to incidents and crises. This framework should include: - policy and minimum standards to drive consistency (including over testing); - clarity over escalation criteria and escalation paths;	**2.1a**	Action: The current Business Continuity Management Policy will be expanded to incorporate the common framework, and rebriefed across the organisation. It will address the points specified by IA. A testing plan will then be developed and executed. Owner & Dept: Head of Department, Operations Services and Procurement, Finance and Operations Date: 31 December 2014

	- tools and templates to support staff in the implementation of responses; - details of how the efforts of different response teams would be co-ordinated; - plans for the production, review and approval of crisis communications; - the assessment of 'near misses' to identify lessons learned; and - post-incident reviews to capture and monitor remediation actions and identify lessons learned.	**2.1b**	Action: Clarity over escalation paths and high level escalation principles will be developed as part of the overarching framework. In line with our stated aim of ensuring that staff continue to exercise their 'judgment' when dealing with issues/events, such escalation criteria will not be able to be exhaustive. Owner & Dept: Head of Department, Operations Services and Procurement, Finance and Operations Date: 31 December 2014

3	**Further work is required to improve the capability of FCA staff members to implement appropriate and timely responses to incidents and crises.**	**Moderate**

The FCA does not have arrangements in place to develop the capability of the organisation to respond to incidents. Organisational capability to respond requires processes that have been tested and people who are practised in responding to likely and extreme scenarios. Based on the documentation reviewed and discussions with stakeholders, we consider that there is limited:

- staff awareness of the FCA's approach to implementing responses;
- understanding of the responsibilities of all individuals in incidents and crisis management;
- training of staff with specific roles in developing and implementing responses; and
- testing arrangements to assess the robustness of the framework and raise staff confidence.

Awareness and training

There is currently no training and awareness programme for staff with roles and responsibilities in the IMF. IMF plans have, however, been walked through with all individuals who have a role in the plans so they are aware of their roles and responsibilities. However, some individuals below the IMT level were not confident of carrying out their roles and responsibilities in the event of an incident as long periods had elapsed since they received training. This would be problematic should the IMF be invoked.

Testing and exercising

During the course of fieldwork, the first testing of the IMT took place with ExCo members. These first tests of the IMF covered a scenario with both a business and operational component but it is unclear how these tests will be extended to the remainder of the organisation. A survey of some staff in the four teams that support the IMT highlighted that most staff desired a practice session where they could work through potential scenarios as a group so that they would be ready to act, in the event of an incident.

We note that further tests are planned for internal teams including Supervision, Markets and Communications & International Divisions in November 2014 and the wider organisation in February 2015.

Recommended outcomes		**Management actions, owner and date**	
3.1	A training and awareness programme is in place to support staff awareness of the FCA's approach to incident response and crisis management. The programme should provide staff with key roles and responsibilities progressively challenging training.	**3.1a**	Action: As per the schedule being developed by the existing business continuity programme a schedule of training and testing exercises will be planned and delivered from 2015 onwards. This will be amended to reflect the changes to the overall framework, the specific scenario of an uncontrolled release of price sensitive information and other scenarios as required. Owner & Dept: Head of Department, Operations Services and Procurement, Finance and Operations Date: 31 December 2015
3.2	Regular testing is undertaken of the FCA's approach to incident response and crisis management and the results of these tests are used to enhance procedures.		See action 3.1a above.

Appendix 1 – findings related to objectives and risks defined during scoping

Objective	Risk	Related findings
To enable the FCA to prepare for, anticipate, respond to and recover from a situation that threatens the organisation's strategic or operational objectives, reputation or viability.	The lack of or inadequate incident response and crisis management capability within the FCA may lead to an ineffective, uncoordinated and / or slow response to a crisis which could have a detrimental impact on the FCA's objectives and reputation.	**Finding 1** – Existing governance arrangements over the organisation's approach to incident response and crisis management are inadequate.
		Finding 2 – The FCA does not have a single overarching framework in place to support staff in implementing effective responses to incidents and potential crisis situations.
		Finding 3 – Further work is required to improve the capability of FCA staff members to implement appropriate and timely responses to incidents and crises.