Financial Conduct Authority

Internal Audit report

The identification, handling and management of market sensitive information

Findings identified	
Major	**1**
Moderate	**4**
Minor	**1**

24 October 2014

1 Executive Summary

1.1 Summary and opinion for Audit Committee

Background

Market sensitive information is described in the FCA Employee Handbook as firm information that could impact share prices or markets. In August 2014, new guidance was provided for the *identification and handling of inside information by the FCA*. Inside information, as defined by Section 118 of the Financial Services and Markets Act 2000, is a subset of market sensitive information and should be classified and handled as Controlled Distribution.

Work performed

Our fieldwork included:

- the performance of Livelink searches with the IS Security Team in the IS Division (the results are set out in Appendix 2),
- interviews with a number of members of FCA staff about various aspects of identifying, handling and managing market sensitive information, and
- the review of policies and training material.

Our testing of local guidance issued by departments for the *identification and handling of inside information by the FCA* focused on departments in the Authorisations, Supervision and Enforcement and Financial Crime Divisions. The Markets Division was excluded from our testing as the UK Listing Authority's controls over market sensitive information were reviewed in the April 2014 Internal Audit review of the UKLA. Actions relating to the need to develop a strategic approach to market sensitive information in the UKLA are due for completion by 30 September 2014.

Conclusions

The FCA staff members interviewed had a consistent and accurate view of what constitutes market sensitive information. A number of those interviewed were also able to clearly articulate examples of how they have handled and managed market sensitive information appropriately. However, our fieldwork has led us to conclude that there is a lack of awareness amongst FCA staff of the risks associated with the handling of market sensitive information. Some FCA staff interviewed were unclear that sending information in the body of emails to firms and other external bodies, excluding the PRA and Bank of England, is not a secure form of communication. They were also unclear whether and how they should indicate to a firm or other body that the information they are sending is market sensitive and should be handled accordingly. The FCA's Senior Leadership Team needs to do more to mitigate the risk that FCA staff members who use or create market sensitive records on a daily basis might become de-sensitised to the nature and sensitivity of the information they are handling.

FCA staff members interviewed as part of this review provided positive feedback about the August 2014 guidance. At the time of our fieldwork, the August 2014 guidance had not yet been incorporated into FCA's policy for *information classification, marking and handling* (hereafter referred to as 'the policy'), nor in local guidance issued by various departments to support this policy. However, we consider that once embedded in this policy and any local guidance, the August 2014 guidance should help increase staff understanding of the identification, handling and management of inside information at the FCA.

We also found that there are weaknesses in departments' local guidance across the board with the exception of the Enforcement Division. Common weaknesses relate to a lack of practical guidance and examples of the ways in which staff can identify, handle and manage market sensitive information. Good local guidance recognises the different uses of information, the different challenges associated with handling records faced by different areas of the FCA and provides guidance to address these challenges.

There is an open risk in the Consolidated Risk Manager (CRM) relevant to the scope of this review - *the risk that information may not be handled securely by members of staff, leading*

to leaks, theft or loss of information (CRM #2703). This risk is owned centrally by the IS Security Team in the IS Division. However, local business areas have not articulated risks or controls relating to the identification, handling and management of market sensitive information as part of their First Line of Defence Attestations. In our view, management in each of the FCA's departments should consider the particular risks presented by the identification, handling and management of market sensitive information and assess the adequacy and effectiveness of controls they have in place to mitigate these risks.

The FCA Executive Operations Committee or another appropriate forum needs to consider the impact of the August 2014 guidance on the open file structure in Livelink. In our view, the August 2014 guidance is likely to result in an increased volume of records needing to be stored in restricted access folders in Livelink. This in turn will lead to an increased administrative burden and will also increase the risks associated with how records are locked down in Livelink currently.

Section 4 of the FCA's Code of Conduct requires FCA staff members to seek prior clearance from their line manager to deal in securities and related investments in Relevant Organisations, which include listed firms and FCA regulated firms. However, there is no monitoring of compliance with this requirement, nor are the managers interviewed aware of what information they need to obtain before they give their staff permission to trade. FCA staff members are also not required to attest to having disclosed all trades in Relevant Organisations to their line manager.

A number of 'business as usual' supervisory records, such as those relating to business model and strategy analysis (BMSA), deep dives, and firm evaluation packs are filed in unrestricted folders in Livelink. In our view, some of these records contain market sensitive information. Management of the Supervision Division needs to do further work to increase supervisors' awareness of the potential for these 'business as usual' supervisory documents to include market sensitive information and of the need for supervisors to handle these documents appropriately.

The FCA needs to ensure that the security vetting of consultants who work at the FCA is equal to the vetting of FCA staff and in line with the requirements in the FCA Employee Handbook.

We have mapped out in Appendix 1 the links between the findings of this review and the risks to the objective we identified in scoping this review.

1.2 Overall management comments

Thank you for the internal audit report on the topic of market sensitive information.

It is imperative for the organisation that 'market sensitive information' is effectively identified, handled and managed by our staff. If we fail to handle this information in an effective manner, we run a number of risks as an organisation, which fall outside of our accepted risk appetite. As such, we take seriously any findings in relation to this area.

We are pleased that the FCA staff members you interviewed had a consistent and accurate view of what constituted market sensitive information. As you have referenced, we have already done significant work to roll out new guidance in this area, but accept that we still have further work to embed this across the organisation and increase awareness of market sensitive information by staff. In addition, we already have staff in the process of visiting management teams to help raise awareness of the importance of handling market sensitive information. We are conscious that the finding around increasing staff awareness is a longer term and on-going issue, which we will continue to work on. We also note that for the FCA to operate efficiently and effectively, it is necessary to strike the right balance between wanting to be a 'knowledge sharing' organisation, and managing the risks around the inappropriate release of sensitive information.

In regards to the other key findings, we note that there exist a number of interdependencies, and we will undertake careful consideration and analysis of what actions to undertake to remediate upon the issues you have identified.

Management agrees with the findings of this report and some of the actions to address them have already been taken or are well advanced. 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 operations committee (EOC) and allow for appropriate consideration of the correct remedial actions and specific consideration of the recommendations in the Davis report.

We also note that similar steps and measures may be needed in respect of other categories of sensitive information e.g. personal data.

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

1.3 Schedule of findings

Ref	Findings	Rating
1	**Awareness and guidance –** There is a need for better awareness amongst FCA staff of the risks associated with identifying, handling and managing market sensitive information. Departmental local guidance has to be improved to help ensure that market sensitive information is identified, handled and managed appropriately by FCA staff.	**Major**
2	**The open file structure in Livelink –** The Executive Operations Committee or other appropriate forum needs to analyse the impact of the August 2014 guidance for the *Identification and handling of inside information by the FCA* on the need to withhold principle applied in Livelink. This analysis is necessary to determine whether the open file structure remains appropriate going forward, and to help ensure that the risks associated with the open file structure are adequately managed.	**Moderate**
3	**The use of encryption to share market sensitive information with firms and other external bodies -** The FCA needs to ensure that confidential and market sensitive information sent to firms or other external bodies via email is appropriately encrypted.	**Moderate**
4	**Trading of securities and investments by FCA members of staff -** There needs to be increased oversight of and strengthened controls over the trading of securities and related investments in Relevant Organisations by FCA staff.	**Moderate**
5	**Identification, handling and management of market sensitive information in the Supervision Division –** Management of the Supervision Division should consider providing further guidance for the identification and handling of market sensitive information in 'business as usual' supervisory documents, such as those relating to business model and strategy analysis (BMSA), deep dives and firm evaluation packs.	**Moderate**
6	**Security vetting of consultants working in the FCA** - The FCA needs to ensure that the security vetting of consultants who have access to FCA information is equal to the vetting of FCA staff and in line with the requirements in the FCA Employee Handbook.	**Minor**

2 Detailed findings

1	**Awareness and guidance**	**Major**

Staff awareness of the risks associated with the handling of market sensitive information requires improvement. In addition, weaknesses in local guidance supporting the FCA's policy for *information classification, marking and handling* need to be addressed.

The need for better awareness of the risks associated with handling market sensitive information

Members of the FCA's Senior Leadership Team and other FCA staff members interviewed felt that there is a need to embed a stronger awareness amongst FCA staff of market sensitive information and the risks to the FCA associated with identifying and handling market sensitive information.

Our sample testing identified records in Livelink containing information, which in our view, is market sensitive. We also found a high number of records marked Controlled Distribution which were not kept in a restricted access folder (further details of our testing are provided in Appendix 2). In our view, there is a significant risk that FCA staff members who create and use market sensitive records on a daily basis could become de-sensitised to the nature and sensitivity of the information they are handling. The Executive Operations Committee or other appropriate forum should consider the following options to mitigate this risk:

- Improving oversight of the risks and controls associated with the identification, handling and management of market sensitive information by including these risks and controls in divisional First Line of Defence Attestations.
- Requiring relevant FCA staff members to attest annually to their understanding of the FCA's policy in respect of the identification, handling and management of market sensitive information. It is common practice in the investment banking industry, regulated by the FCA, for firms to ask employees to attest annually to their understanding of the firms' policies.
- In our view, the FCA's Senior Leadership Team should make more explicit the link between the FCA's cultural characteristic of *Professional Excellence* and the requirement to manage records appropriately, for example, in staff performance plans and reviews.
- Strengthening the induction of new starters by emphasising the risks associated with the identification, handling and management of market sensitive information. The online training provided to new joiners on Livelink also requires improvement as this training needs to instruct FCA staff members on how to restrict access to records in Livelink.
- Ensuring that the FCA's Senior Leadership Team leads by example. We were told that there were instances where members of the FCA's Senior Leadership Team sent internal emails containing market sensitive information without the appropriate classification.
- Providing presentations to all local areas on information classification, including the risks associated with identifying and handling market sensitive information. Presentations by the General Counsel's Division and the IS Security Team to local areas were found to be helpful in raising awareness of the importance of handling records appropriately.

Most FCA staff members interviewed stated that if they are unsure if a specific piece of information is market sensitive, they would consult their line manager or Head of Department. However, we found examples of FCA staff members, outside of the Markets Division, who expect staff in the Markets Division to decide whether the information is market sensitive on their behalf. As identifying market sensitive information may be challenging for staff, relevant divisions should have local champions in place who have the authority and technical knowledge to train and advise staff on how to identify and manage market sensitive information.

The need for improved local guidance

Departments across the FCA have created their own local guidance supporting the FCA's policy for *information classification, marking and handling.* Local guidance for information classification, marking and handling is important as it recognises the different uses of records and the challenges associated with handling records in different areas of the FCA. We recognise that, at the time of our fieldwork, local management teams across the FCA had not incorporated the August 2014 guidance into local guidance. However, we understand there are plans in place to do so.

We reviewed the local guidance issued by a sample of FCA departments and found that improvements are needed to address the following issues:

- With the exception of the local guidance for the Enforcement Division, the local guidance for other departments did not provide relevant local examples of market sensitive records, nor provide guidance on how to overcome specific challenges faced by the local areas in the handling and management of local market sensitive records.
- FCA staff members interviewed raised practical challenges to handling and managing records classified as Controlled Distribution which include market sensitive records. The FCA's policy for *information classification, marking and handling* should be enhanced to help support FCA staff members with the practical challenges of handling and managing Controlled Distribution records, for example:
    - how to label and treat internal emails which contain information classified as Controlled Distribution; and
    - whether and how to maintain records of who information classified as Controlled Distribution had been shared with.

  We were told of instances where Controlled Distribution records that had been restricted and managed appropriately locally were then distributed to other FCA members of staff outside of the initially identified need to know group. There is also no monitoring of who the information is shared with.
- The FCA's policy for *information classification, marking and handling* should also make clear that responsibility for the identification, marking and handling of market sensitive information rests with the FCA department which created the information.
- Local department guidance should make clear that the responsibility for determining the appropriate classification of FCA committee papers rests with the authors of those papers. FCA staff members interviewed felt that the application of the Controlled Distribution classification to some FCA committee papers was not done with regard to the sensitivity of the information in these papers.
- FCA staff members interviewed questioned whether they are required to declassify a record which is no longer market sensitive and how to do this. Our review of a sample of records on Livelink found a number of records that were no longer market sensitive but which were still marked as Controlled Distribution. Local department guidance should set out an agreed approach to this.
- The Bank of England and PRA have their own set of information classifications. Local department guidance for all the FCA departments we reviewed states that information received from the Bank of England or PRA, which is classified as Bank Confidential, should be treated as Controlled Distribution. However, FCA staff members interviewed commonly handled Bank Confidential information as FCA Restricted. Clarification is needed in the policy to require Bank Confidential information to be handled as Controlled Distribution and local department guidance updated accordingly.
- A number of FCA staff members interviewed were unclear where to source their local department guidance for *information classification, marking and handling* and felt that clear links to this guidance should be made available on the intranet.

Recommended outcomes		**Management actions, owner and date**	
1.1	FCA staff members are made aware of the risks associated with handling and managing market sensitive information e.g. through the provision of induction and refresher training which would include escalation paths to local champions and line management. This awareness is maintained.	**1.1**	Action: EOC will be provided with a paper for discussion of remedial actions to meet this recommended outcome. Some changes to induction and training have already been made, and actions to raise awareness with management teams are in hand. EOC will review proposals for further changes to induction and on-going awareness initiatives. This will include consideration of controls such as mandatory training or an attestation process. Following the EOC review, it will be necessary to

			produce a detailed plan for execution of any follow-on actions. **Owner & Dept:** COO **Date:** 30 November 2014
1.2	Local guidance on *information classification, marking and handling* for all departments across the FCA is improved to cover the points raised in this finding. FCA Staff members are aware of the local guidance and where to find it.	**1.2**	Action: The production / refresh of department specific information classification guidance notes is underway in the business. The guidance notes will then be promoted to staff within each department. Each guidance note will have a business owner who is responsible for ensuring the document is updated when appropriate. The COO's office and the Information Security team will monitor the initial production and promotion of the first set of guidance notes. Awareness of local guidance will be reflected in induction and refresher training for staff. Following EOC discussions, the guidance notes may require revision and it may therefore be necessary to raise follow-on actions to take account of this. **Owner & Dept:** COO **Date:** 31 Dec 2014

2	**The open file structure in Livelink**	**Moderate**

An assessment is required of the impact on the open file structure in Livelink following the issuance of the August 2014 guidance for the *identification and handling of inside information by the FCA.*

The open architecture in Livelink

The file structure in the FCA's electronic document and records management system, Livelink, is largely open and follows the principle that access to folders is only controlled where there is a need to withhold information. This open structure allows access to information across the organisation or to all system users in one or more divisions, with the exception of some folders where access has been locked down to specified groups of named system users. We understand that the decision to have this open structure in Livelink and its predecessor system, the T: Drive, was made in April 2004 and was driven by the desire to work collaboratively and share information across the organisation.

Restricting access to market sensitive information in Livelink

The FCA's policy for *information classification, marking and handling* in the FCA Employee Handbook requires that market sensitive information be classified as Controlled Distribution. The Handbook further requires that this information which is stored in Livelink should be filed in folders with access restricted to those who have a proven need to know. In August 2014, management issued new guidance for the *identification and handling of inside information by the FCA* which provides further clarity over when information is inside information and which should then be classified as Controlled Distribution. The guidance also emphasises the need to handle this information carefully.

Potential impact of the August 2014 guidance on Livelink

The proper application of the August 2014 guidance is likely to result in an increased volume of documents being treated as Controlled Distribution and being stored in locked down files in Livelink. In our view, the need to handle and manage an increased volume of documents as Controlled Distribution could lead to (1) an increased administrative burden, and (2) increased risks associated with the locking down of information in Livelink, in particular, the risk that local awareness of records that have been locked down may decline if staff members with access to the information were to leave the FCA. However, as yet, no analysis of the impact of this has been performed to determine the administrative costs and the increased risks associated with locking down more records.

The Executive Operations Committee or other appropriate forum may need to consider whether moving away from a need to withhold principle to a need to know principle, where files are only unlocked where there is a proven need to share information, might be appropriate going forward in Livelink.

We raise the following opportunities to strengthen controls to address the increased risks associated with the locking down of information in Livelink:

- Use of the categorisation tool for documents in Livelink which enables documents to be categorised as Controlled Distribution thereby improving the ability to track and provide oversight of these records.
- Further strengthening of the central programme of records management testing. For example, performing tests to confirm whether all areas of Livelink are covered by the testing performed by local areas. Management should also take this opportunity to review whether the current tolerance level of 3% for non-compliance with the policy of locking down records marked as Controlled Distribution is too high given that this classification includes market sensitive information.

Recommended outcomes		Management actions, owner and date	
2.1	The Executive Operations Committee or other appropriate forum analyses the impact of the August 2014 guidance on the need to withhold principle applied in Livelink and ensures that if the open file structure is to remain, there are adequate resources and controls in place to help ensure that market sensitive information is handled and managed appropriately.	**2.1**	Action: 'FCA Restricted' is the FCA's default classification and is based upon the 'need to withhold' principle. The 'need to know' principle is an explicit part of the "Controlled Distribution" classification. EOC will consider the impact of the new guidance on the FCA's Records Management policy and the file structure within Livelink. EOC will also consider additional resources or controls that maybe required as a result of the practical effects of the agreed policy and associated risk tolerances. Following the EOC review, it will be necessary to raise risks and / or follow-on actions. **Owner & Dept:** COO **Date:** 30 November 2014

3	**The use of encryption to share market sensitive information with firms and other external bodies**	**Moderate**

Members of staff across the FCA are required to email firms and other external bodies on a regular basis to obtain and share information in order to perform their role effectively. However, there are risks associated with emailing information that is market sensitive, or more broadly, information that meets the classification of Controlled Distribution, to firms and other external bodies. This may include the following risks:

- A sender can easily email market sensitive information to the wrong person or address by mistake; and
- Sending firms and other bodies, excluding the PRA and Bank of England, information via email is not a secure form of communication as emails can be intercepted or accessed once sent outside the FCA.

Encrypting emails would help to mitigate the risks of sending information to the wrong email address or of emails being intercepted as these encrypted emails can only be accessed by a recipient in possession of the required password or key. The majority of FCA staff members interviewed are aware of the need to encrypt data and other attachments containing market sensitive information before sending this information to firms or other external bodies via email. However, a number of these interviewees had not thought about encrypting market sensitive information contained in the body of an email.

One of the supervisors interviewed noted that their supervision team was installing PGP (Pretty Good Privacy), a data encryption and decryption computer program for email, and arranging with the supervised firm to also install PGP for future communications. This supervisor stated that it had been challenging to have PGP installed and it was not clear to them whether the installation of PGP was required for all supervisory teams. We are aware that the IS Technology Security Team is piloting an alternative secure email system. Further work is needed to identify a user friendly encryption tool. Management of the Supervision and Authorisations Divisions in particular should ensure that all teams utilise appropriate encryption tools for emails.

We also found that some members of staff interviewed were unclear about whether they are required to and how they should indicate to a firm or other external body that information sent via email is market sensitive and should be handled accordingly by that firm or external body.

Recommended outcomes		**Management actions, owner and date**	
3.1	Firms and other external recipients of information are made aware about the sensitivity of any information that is communicated to them and how this information should be handled.	**3.1**	Action: The use of FCA classification markings for documents sent outside of the FCA is not suitable as the FCA scheme is not used or understood elsewhere. Therefore, it is necessary for staff to inform external recipients about the sensitivity of the material – this is an inherent risk that must be accepted and managed. Accordingly we believe we have already raised awareness of this issue through the process of visiting management teams on the subject of market sensitive information. To further manage this risk, Information Security will investigate the feasibility of applying an automatic cover note to external email to explain the recipient's responsibilities when handling FCA information. The review of local guidance will also enforce this issue.

			Owner & Dept: Chief Information Security Officer, IS Information Security **Date:** 31 January 2015
3.2	Confidential or market sensitive information is not sent to firms or other bodies without the appropriate security to protect the information.	**3.2**	Action: Secure external email cannot be achieved in all cases as it requires actions by the other party. In some circumstances, it will not be possible to encrypt email and the risk will therefore need to be accepted. However, the importance of using current IS services, where feasible, will be reinforced as part of the awareness raising initiatives. The current IS services for secure email (PGP and encrypted Winzip) are suitable for some circumstances, but are not fit for purpose in others. Information Security will therefore pilot an alternative secure email 'portal' service with business users to determine whether it is appropriate for FCA users. Following a pilot, it may be necessary to raise follow-on actions to track further deployments and promotion of the service, if the pilot is successful. **Owner & Dept:** Chief Information Security Officer,IS Information Security **Date:** 30 April 2015

4	**Trading of securities and investments by FCA members of staff**	**Moderate**

Section 4 of the FCA's Code of Conduct on *personal dealings in securities and related investments* requires FCA staff members to seek prior clearance from their line manager to deal in securities and related investments in Relevant Organisations[1]. However, there is no monitoring of compliance with Section 4 of the FCA's Code of Conduct. In addition, a number of the FCA line managers we interviewed were not aware of what information they should obtain before they give line reports their permission to trade, although there is online guidance available to line managers about this. Furthermore, although members of staff are required annually to update their disclosure of interests and confirm compliance with the Bribery Act, FCA staff members are not required to attest that they have complied with Section 4 of the FCA's Code of Conduct.

There were 434 requests from FCA staff seeking line manager approval to deal in securities and related investments in Relevant Organisations between 1 August 2013 and 18 August 2014. Of these, 101 related to requests to deal in securities of FCA regulated firms. Our testing found market sensitive information relating to firms was stored in open areas of the firms and groups area of Livelink and would be available to some FCA members of staff who received permission to trade.

The Corporate Services Department is currently scoping a planned review of the FCA's Code of Conduct and the associated processes. The following points should be considered as part of this review.

Monitoring of compliance

Currently, line manager clearance is sought and given via a form submitted in the Chrysalis system by the FCA staff member wishing to buy or sell securities or related investments in Relevant Organisations. While the Corporate Services Department is able to obtain reports from Chrysalis of the trades that individuals have submitted for approval, it does not perform any active monitoring or testing of compliance with Section 4 of the FCA's Code of Conduct.

The Conduct of Business (COBS) section of the FCA Handbook requires FCA regulated firms to have adequate arrangements in place to prevent individuals with access to inside information from entering into personal transactions which would involve the misuse of this inside information. The Systems and Controls (SYSC) section of the FCA Handbook requires FCA regulated firms to monitor the effectiveness of these arrangements. We, therefore, consider that the FCA would be expected to monitor compliance with Section 4 of the FCA's Code of Conduct. In our opinion, monitoring of compliance with Section 4 of the FCA's Code of Conduct could be performed by sampling a selection of trades that FCA staff members have sought approval for in the Chrysalis system.

Guidance for line managers on providing permission to trade

When submitting an online request to trade to their line manager, the FCA staff member is required to confirm on Chrysalis that they have not had access to any inside information. The Chrysalis system then requests line managers to respond to the requests in a short timeframe. The August 2014 guidance for the *identification and handling of inside information by the FCA* will help increase FCA staff members' understanding of what constitutes inside information and should therefore help a staff member and their line manager to judge whether or not a staff member seeking to trade has had access to inside information. However, the open access structure in Livelink may mean that an FCA staff member has access to more information than their line manager may be aware of. The Executive Operations Committee or other appropriate forum should therefore review the policy and guidance for line managers on what trading might be considered appropriate by FCA staff members, for example, through the provision of a restricted list of companies that FCA staff members cannot deal in. It is common practice in FCA regulated firms for there to be a restricted list of securities which employees are restricted from buying or selling.

[1] The FCA's Code of Conduct defines Relevant Organisations as those companies, or any company within the same group of companies, either seeking to be or currently listed, or otherwise publicly traded in the UK and/or quoted and/or regulated in the UK as appropriate

Attesting to compliance

FCA staff members are not required to attest that they have disclosed all trades in securities and related investments in Relevant Organisations to their line manager. In our view, adding this attestation to the annual Code of Conduct submission for all FCA staff members would help to increase staff awareness of the requirements of Section 4 of the FCA's Code of Conduct.

Recommended outcomes		Management actions, owner and date	
4.1	Responsibility for monitoring compliance with Section 4 is assigned to a department. Compliance with Section 4 of the FCA's Code of Conduct is monitored.	**4.1**	Action: Monitoring compliance effectively could be challenging without significant time, resource and specific expertise and even then, may not identify if anyone were to be purposefully trying to deal in contravention of the Code. This raises the bigger question of the purpose of the Code and whether it represents a meaningful control. Corporate Services will consider monitoring of compliance as part of their current review of the code of conduct. Following this review, proposals will be submitted to ExCo In the meanwhile, ExCo has indicated that it is supportive of extended attestations, as noted in 4.3 below. **Owner & Dept:** Company Secretary, Corporate Services **Date:** 31 March 2015
4.2	There is appropriate guidance for line managers as to what trades are appropriate and what information they should obtain before they give line reports their permission to trade. Line managers are aware of the guidance and where to find it.	**4.2**	Action: Specific guidance for line managers was produced by Corporate Services and published on My FCA Hub last year. This will be reviewed and re-publicised to line managers. Consideration will also be given to re-issuing the guidance, perhaps as a laminated card for ease of reference. There may also be merit in a wider communication to all staff of things to consider before dealing, perhaps via the Hub. **Owner & Dept:** Company Secretary, Corporate Services **Date:** 31 March 2015
4.3	FCA staff members are required to attest that they have complied with Section 4 of the FCA's Code of Conduct.	**4.3a**	Action: In the short term, we believe there would be merit in seeking annual attestations but, as it is not possible to amend Chrysalis in time for the annual review of the Code which is due shortly, we propose introducing an attestation for SLT members this year to be done by email. **Owner & Dept:** Company Secretary, Corporate Services **Date:** 31 December 2014
		4.3b	Action: A longer-term solution that can be applied to all staff will be investigated through amending Chrysalis or, ideally via the PeopleHub. This will be considered as part of the current review of the code of conduct. Following this review, proposals will be submitted to ExCo (also see action 4.1).

			Owner & Dept: Company Secretary, Corporate Services **Date:** 31 March 2015

5	**Identification, handling and management of market sensitive information in the Supervision Division**	**Moderate**

Supervisors routinely handle and manage a large amount of market sensitive information, particularly those supervisors who supervise C1 and C2 firms. During our fieldwork, we found examples of supervisors identifying and handling as market sensitive information relating to ad-hoc events, such as an enforcement case and interim results announcement and labelling this information appropriately as Controlled Distribution. However, the supervisors interviewed did not classify and handle 'business as usual' supervisory documents, such as those relating to business model and strategy analysis (BMSA), deep dives and firm evaluation packs, as containing market sensitive information.

We found a number of these types of documents stored in Livelink folders open to other members of the Supervision and Authorisations Divisions. Specifically, we found BMSA documents for two C1 firms which contained analysis of financial information and product strategies, documentation relating to two deep dives for two C1 firms, and a paper discussing why another listed firm was included on the watchlist in open Livelink folders. In our view, the content of these documents meets the definition of inside information set out in the FCA's August 2014 guidance on the *identification and handling of inside information by the FCA* and should therefore be handled and managed as Controlled Distribution.

Whilst we recognise that the identification of market sensitive information is a subjective decision and is ideally made on a document by document basis, we consider that further work is needed by the management of the Supervision Division to increase the awareness of the potential for supervisory documents to include market sensitive information and the need to treat market sensitive information as Controlled Distribution. The management of the Supervision Division should consider, for example, whether to provide divisional guidance on the handling of these 'business as usual' supervisory documents. This guidance could be provided as part of the required updated local guidance discussed in finding 1. This would help ensure that inside information is recognised as such and handled appropriately.

Recommended outcomes		**Management actions, owner and date**	
5.1	Market sensitive information contained in firm evaluation packs, BMSA and other standard documentation held by the Supervision Division is identified, handled and managed appropriately and in accordance with FCA policies and guidance.	**5.1a**	We note the findings on identification, handling and management of sensitive information in Supervision Division. We will review our guidance in coordination with a wider review of FCA policy on the appropriateness of an open Livelink architecture and a philosophy of sharing information across the FCA. We will look further at the advantages and disadvantages of accessibility of documents to FCA to staff to enable them to do business (e.g. deeming all FCA staff as 'insiders') versus limiting access to sensitive information (or subsets of such information) to defined user groups. We will revise and/ or supplement guidance to: assist staff in their understanding of our policy, increase their awareness of the types of documents that may include market sensitive information, and provide consistency in approach

			across the Division. Action: Review and amend/ supplement guidance on identification and handling of market sensitive information. Roll out guidance in Supervision Division. **Owner & Dept:** Head of Central Support, Supervision **Date:** 31 December 2014
		5.1b	Action: Work with sub-Divisions and Directors to ensure that the guidance is understood and embedded in local areas. Identify any further actions that may be required to achieve the intended outcome. **Owner & Dept:** Head of Central Support, Supervision **Date:** 31 March 2015

6	**Security vetting of consultants working in the FCA**	**Minor**

At the time of fieldwork, testing was required of some consultancy firms' staff security vetting policies to ensure they meet the expected FCA standards.

The FCA currently uses the services of consultancy firms, and staff from 12 of these firms are exempt from being security vetted through the FCA's processes. The on-boarding and security vetting for staff from other consultancy providers is currently undertaken by the FCA's outsource provider for recruitment and on-boarding.

We understand from the Procurement Department in the Finance and Operations Division that the requirement to adhere to all relevant FCA policies is documented in contracts between the FCA and each of these 12 consultancy firms. Compliance with the FCA Employee Handbook requires staff to undergo pre-employment checks which incorporate all elements of the *Government Baseline Personnel Security Standard* checks.

However, the FCA does not perform tests to confirm whether staff members of these 12 consultancy firms are vetted in line with the requirements in the FCA Employee Handbook.

This issue was highlighted at the Operational Security Group meeting of 6 August 2014 where an action was assigned to ascertain whether compliance sample tests would be permissible. We understand that the Corporate Protection & Resilience Team is currently drafting a proposal for compliance sample tests to be undertaken going forward.

Recommended outcomes		**Management actions, owner and date**	
6.1	Compliance tests are undertaken to validate whether staff of consultancy firms have been security vetted in line with the requirements of the FCA Employee Handbook.	**6.1**	Action: We agree that compliance testing of vetting standards should be undertaken on a proportionate basis going forward. A paper will go to the Operational Security Group (OSG) in the near future for a decision on the frequency and manner of supplier compliance checks that should be carried out, including in relation to the 12 firms identified by IA. OSG will also decide upon who should own this process. Following OSG's decision, further actions will be required to set out the implementation of the compliance checks. **Owner & Dept:** Security Manager, Operations Services **Date:** 31 October 2014

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

Objective	Risks	Related findings
To prevent the inappropriate use or disclosure of market sensitive information.	The risk that the FCA or a member of its staff uses or discloses market sensitive information inappropriately as a result of not recognising or identifying market sensitive information.	**Finding 1** – The FCA's policy for the *information classification, marking and handling* and the FCA departments' local guidance, supporting this, needs to be improved to cover the identification of market sensitive information, as well as to cover in better detail the practical challenges of handling this. **Finding 3** - The FCA needs to advise firms and other recipients about the sensitivity of any information it communicates to them and how this information should be handled.
	The risk that the FCA or a member of its staff uses or discloses market sensitive information inappropriately as a result of not storing market sensitive information securely or sharing/releasing market sensitive information inappropriately, either in the FCA or to other external bodies.	**Finding 1** - There is a need for better awareness amongst FCA staff of the risks associated with market sensitive information. **Finding 2** – The Executive Operations Committee or other appropriate forum needs to analyse the impact of the new August 2014 on the need to withhold principle applied in Livelink to determine whether the open file structure remains appropriate and the risks associated with this are adequately managed. **Finding 3** - The FCA should not email market sensitive information to firms or other external bodies without appropriate encryption to protect the security of this information. **Finding 4** – There needs to be increased oversight for, and strengthened controls over, the trading of securities and related investments in Relevant Organisations by members of FCA staff. **Finding 5** – Management of the Supervision Division should ensure that market sensitive information contained in 'business as usual' supervisory documents is handled appropriately.
	The risk that the FCA or a member of its staff uses or discloses market sensitive information inappropriately as a result of the ownership or expected management of market sensitive information not being clear throughout the course of its lifecycle.	**Finding 1** – The FCA's policy for the *information classification, marking and handling* and the FCA departments' local guidance supporting this, needs to be improved to include making it clear that the identification, marking and handling of market sensitive information is the responsibility of the department that created it. **Finding 2** – Given the expected increased volumes of records in Livelink which will need to be restricted, strengthened controls are needed to help mitigate the risks associated with how records are managed in Livelink currently.

Appendix 2 – Additional information

As part of our fieldwork, we found there were an estimated 42,000 records in Livelink, including records restricted to limited user groups, that contained the phrase 'Controlled Distribution'. An estimated 4,500 of these records were open to all staff users of Livelink, and 7,500 were open to members of Internal Audit. The results of the Livelink searches conducted by the Records Management Support Team in the IS Division and by the Internal Audit Division included all records which included the term Controlled Distribution. The records found include training and guidance material as well as records considered and classified as 'Controlled Distribution'. The Livelink searches that were performed searched for records added between 1 April 2013 and September 2014.
The management information provided to the Records Management Operations Group shows compliance with the FCA's policy of keeping Controlled Distribution records in restricted access folders is exhibiting a downward trend, and in June 2014 was only marginally above the pre-set target of 97%. The management information is produced from regular compliance checks by departmental Records Management Contacts who test that records classified as Controlled Distribution are not stored in open access areas of Livelink.