Financial Conduct Authority

Internal Audit report

A review of the adequacy and effectiveness of controls for Software Asset Management (SAM)

Findings identified	
Major	**4**
Moderate	**1**
Minor	**0**

12 August 2014

1 Executive Summary

1.1 Summary and opinion for Audit Committee

The FCA has a large and diverse software estate, including over 340 desktop applications, which is managed by the Software Asset Management (SAM) process. This is the process by which software assets and the associated licence and 'support and maintenance' contracts are managed throughout their lifecycle. SAM helps to ensure that an organisation is compliant with its software licence obligations and obtains value for money from its licensing arrangements. Fujitsu is primarily responsible for operating the FCA's SAM processes and for advising the FCA on whether the FCA is compliant with its software licence obligations. The FCA's SAM function, which is part of the Technology Operations department in the IS & PMG Division, is responsible for managing Fujitsu's delivery of SAM processes. The FCA is also responsible for pursuing value for money from its licensing arrangements.

We identified some areas of good practice in the FCA's SAM capabilities. For example, the process for managing licences before, during and after legal cut-over from the FSA to the PRA and FCA was robust; licences were novated or subject to changes that reduced compliance risk.

However, we concluded that the FCA's SAM function does not have a clearly defined direction, strategy or role outside of ensuring software licence compliance. We concluded that a clearly defined remit for the SAM function within the FCA is lacking, there is a lack of strategy for engaging with third-parties for SAM-related activities; and the SAM function does not have the capability to meet its operational requirements. In addition, the SAM function has not documented its objectives and as such its First Line of Defence attestation does not articulate risks to meeting its objectives. Instead, the Directors First Line of Defence attestation focused on 'zero-level' processes, from which controls are articulated. Although we reached agreement with management on the objectives and risks to the function as part of our scoping process, failure to consider objectives and the risks to meeting them is a missed opportunity to identify control weaknesses. We have identified findings against all but one of the risks to the objectives that we identified as part of the scoping process. We have raised a Major finding to address this and identified a number of additional findings that, at the time of our review, impact the agreed risks to the two objectives of the SAM function which we outline below:

Objective: To ensure effective management (including monitoring) of Fujitsu in its capacity as a outsourced SAM service provider

We concluded that there is insufficient internal FCA expertise to interpret, challenge and validate reports, data and information received effectively without significant external assistance.

As a result of the above, we raised three further Major findings with regard to

- insufficient FCA SAM expertise to interpret the information received; and
- the FCA's SAM practices not delivering value for money.

We also raised a Moderate finding.

1.2 Overall management comments

Tech Ops and IS Procurement accept the findings in this report.

However we would like to add that improvements have already taken place, in particular the resourcing of an experienced SAM Manager, and that there are plans in place to address failures identified in this report. In particular we would like to state the following;

1. The remit of the FCA's SAM function: The scope of SAM services, whether provided internally or via 3rd party suppliers is being reviewed and updated with the latest requirements of the industry. We are utilising internal and external resource in order to ensure that the remit is relevant and can be managed going forward as external forces demand change.

2. Utilisation of 3rd Party Suppliers and Monitoring of Performance: Although formalised measurements and KPI's need to be developed, the FCA now has the necessary expertise to assess when third-party assistance is required for SAM, and to make a judgement on the performance of said third-parties. This has already been demonstrated over the management of the contract with Fujitsu, and the cancellation of the SAM review.

3. The FCA's SAM practice delivering Value For Money: The FCA SAM function has improved its focus on providing Value for Money services since the time that the report was written. This has been demonstrated in the cancellation of the SAM Review, and the planning and subsequent delivery of the mitigation plan in order to address the compliance risks with the current licensing. Whilst not all of the risk will be able to be mitigated, without the need to purchase licenses, it is expected that about one third of the current exposure level will be removed, and when the purchase is made it will be with future planning in mind.

IS is constrained by the Fujitsu agreement and the charging mechanisms negotiated. Internal audit have drawn conclusions that the transaction fee for processing purchases does not represent value for money (VfM) but does not suggest why this is the case nor reference the VfM clauses that are set out in the Fujitsu procurement tower. It should also be noted that the FCA is not contractually obliged to utilise Fujitsu to purchase licenses.

1.3 Schedule of findings

Ref	Findings	Rating
1	**The remit of the FCA's SAM function is not defined** In order to operate effectively a Software Asset Management (SAM) function needs to have a clearly defined remit within an organisation. We concluded that the FCA's SAM function does not have a clearly defined remit for the role the SAM function plays within the FCA, there is a lack of strategy for engaging with third-parties for SAM-related activities, and the SAM function does not have the internal capabilities to meet its operational requirements. The FCA As a result, there is a risk that value for money is not achieved as roles within SAM are duplicated. Further, the FCA has not clearly defined the objectives of its SAM function and as such has not considered and defined the risks that may prevent it from meeting its objectives. Instead, the Directors First Line of Defence attestation focused on 'zero-level' processes, from which controls are articulated. This is a missed opportunity to identify mitigation that may have prevented the issues identified in this report from occurring	**Major**
2	***[Commercially Confidential]***	**Major**
3	**The FCA does not have sufficient internal SAM expertise to interpret the information received** The FCA does not have sufficient internal SAM expertise to interpret and challenge the reports.	**Major**
4	**The FCA's SAM practices do not deliver value for money** In addition to its compliance responsibilities, one part of the FCA SAM function's objectives should be to facilitate value for money delivery and to deliver a material return on investment. However, we identified a number	**Major**

	of areas within the SAM processes at the FCA that are not delivering value for money.	

5	***[Commercially Confidential]***	**Moderate**