payments and crypto network

Governance arrangements

A series of guides addressing the subject of governance arrangements for UK authorised Electronic Money Institutions ("EMI") and Payment Institutions ("PI").

Guidance is provided for firms and is not intended as legal advice.

Guide 3: Internal audit arrangements

Background

UK authorised EMI and PI businesses must adhere to the regulatory requirements defined in the Electronic Money Regulations 2011 ("EMR") and the Payment Service Regulations 2017 ("PSR") as well as and associated guidance from the UK's Financial Conduct Authority ("FCA").

The EMR and PSR require firms to maintain *"robust governance arrangements"*, including *"a clear organisational structure with well-defined, transparent and consistent lines of responsibility"*, which are *"comprehensive and proportionate to the nature, scale and complexity of electronic money to be issued and payment services to be provided".*

FCA guidance states that, depending on the nature, scale and complexity of the business, *"it may be appropriate for a firm to maintain an internal audit function which is separate and independent from the other functions and activities of the firm"*.

EBA Guidelines, which also apply to UK authorised EMI and PI businesses, also reference internal audit requirements, specifically (i) EBA Guidelines on ICT and security risk management, and (ii) EBA Guidelines on Outsourcing Arrangements. These guidelines require the scope of internal audit to include ICT and security risk and outsourcing arrangements.

Given the increasing prominence of internal audit within both FCA guidance and EBA Guidelines, it is becoming increasingly difficult for firms to maintain a position that it is not appropriate to maintain an internal audit function. The ability for firms to outsource the internal audit function, rather than maintain internal resources, in whole or part, also points towards an expectation that firms will have some form of internal audit function in place. The FCA's requirement for an annual safeguarding audit should also now be considered as well.

Internal audit should be considered as part of a firm's governance arrangements and is discussed in this guidance.

Definition of internal audit

The internal audit function should work to assess, and make recommendations for the improvement, of the effectiveness of the firm's risk management, internal controls, compliance arrangements, governance processes, and IT and security. The function should maintain its independence from the business and the functions that it audits, enabling it to provide objective findings and recommendations. Outsourcing an internal audit function, in whole or part, is therefore a useful option to achieve the level of 'independence'.

Role of internal audit

The internal audit function would be responsible for examining and evaluating the firm's internal controls, processes, and systems to ensure that they are operating effectively and efficiently, including:

- Providing independent assurance on the effectiveness of the organization's risk management, control, and governance processes
- Assessing the adequacy and effectiveness of the organization's internal control systems; and
- Identifying opportunities for improvement in the organization's processes and controls.

The FCA would expect the internal audit function to have the following responsibilities:

- Establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the firm's systems, internal control mechanisms and arrangements
- Issue recommendations based on the result of work carried out
- Verify compliance with those recommendations; and
- Report internal audit matters to the Board and relevant Board-level Committees (e.g. Audit Committee).

Independence of internal audit

The internal audit function should be independent of the business units that are subject to audit and should report to the Board and / or relevant Board-level Committees. The internal audit function is expected to be objective and unbiased in their work and to provide an independent assessment of the firm's risks, controls, compliance and governance processes. The value that an internal audit function adds to the business is underpinned by its independence.

EBA Guidelines

EBA Guidelines apply to EMI and PI firms and reference internal audit activities, including:

- EBA Guidelines on ICT and security risk management, state that a firm's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks, providing independent assurance of the effectiveness to the Board. The frequency and focus of these audits should be commensurate with the relevant ICT and security risks.

- EBA Guidelines on outsourcing, state that the activities of the internal audit function should cover, following a risk-based approach, the independent review of outsourced activities.

Resourcing internal audit

The majority of EMI / PI businesses will outsource their internal audit function in order to ensure that the function can operate in an independent manner and that it has appropriate expertise available to address the scope of the audit work - for many firms it is difficult to find internal resources that are both independent and who have sufficient expertise to audit all of the areas within scope.

Outsourcing could take place within the group, e.g. to a parent entity that has the required resources and already audits other group companies, or to a specialist third-party outside the group. It would also be possible to outsource to a number of different parties in order to build the required expertise for the scope of work required, for example, specialist IT auditors could be used to supplement the work of a specialist compliance auditor. Outsourcing can also be a cost-effective solution to access experts with specialised skills.

Reporting lines of internal audit

The internal audit function would typically report to the Board, the Audit Committee (if one is maintained), or both. This is because the internal audit function should operate as an independent and objective function and should therefore be free from interference in order to be able to carry out its work effectively. By reporting to the Board or the Audit Committee, the internal audit function can provide assurance that it is independent and objective.

Internal audit processes

The internal audit process should follow a methodology based on a number of pre-defined steps:

1. **Planning**: The internal auditor specifies the scope of the audit work to be conducted during the visit, determines the audit objectives, and develops an audit plan. The audit plan for the visit might be part of an 'internal audit plan' that covers a longer period of time and which has been prepared in consultation with the firm (see below).
2. **Fieldwork**: The internal auditor collects data and evidence to test the effectiveness of the firm's controls and processes. This may include reviewing documents, observing processes, discussions / interviews with staff and testing transactions.
3. **Reporting**: The internal auditor prepares a report that summarises the findings of the audit and provides recommendations for improvement. These are often prioritised according to their risk in order for the firm to prioritise remedial actions.
4. **Follow-up**: The internal auditor follows up on the actions taken to address the recommendations and to ensure that they have been effectively implemented. This step would likely involve the activities described at the 'Fieldwork' stage, i.e. reviewing documents, observing processes, discussions / interviews with staff and testing transactions.

Internal audit charter

This is a document that outlines the purpose, authority, and responsibilities of the internal audit function. It also defines the scope of the internal audit function, including the types of activities that will be audited and the processes that will be followed. An internal audit charter could be prepared to define the responsibilities of the internal audit function (for internal organisation purposes) and for inclusion in any internal audit outsourcing agreement (e.g. as part of a service description to govern service delivery).

Internal audit plan

This is a document that outlines the specific audit engagements that will be conducted by the internal audit department in a given time period. The plan is typically developed based on a risk assessment of the firm's operations and should be subject to review and approval by the Board or Audit Committee (if one is maintained).

An internal audit plan could be developed to cover a longer period of time, e.g. three years, to help resource planning and pro-active resolution of known issues ahead of the internal audit work being conducted.