J Cassidy Business Focus Limited
https://www.jcbfl.co.uk
jane.cassidy@jcbfl.co.uk
+44 (0) 7717 705054 or +44 (0) 1920 872324
Registered in England & Wales - Reg. No. 11370541
Reg. Office: 69b The Maltings Business Centre, Roydon Road, Stanstead Abbotts, Hertfordshire SG12 8UU

Internal Audit Financial Services Code of Practice

Guidance on effective internal audit in the financial services sector

	Level 1 Informal: The IA activity is ad hoc or unstructured. No professional practices have been established, and there is an absence of infrastructure.	**Level 2 Defined:** The IA activity has established and is maintaining the repeatability of processes. There is partial conformance to the IIA Standards, and appropriate reporting relationships established.	**Level 3 Integrated:** Policies and procedures are defined, documented, and integrated into the culture of the IA activity.	**Level 4 Managed**: IA activity is recognized as a significant contributor to the organization. Performance metrics are in place to measure and monitor IA performance. IA is a well-managed business unit.	**Level 5 Optimised:** World-class. The IA activity has acquired top-level professional and specialized skills, and is a critical part of the organization's governance structure	**Evidence**	**Document reference**	**Audit Committee sign-off**	**GAP**	**Rectification**	**Timetable**
Introduction											
The purpose of the Code 1. The recommendations which follow are aimed at enhancing the overall effectiveness of internal audit, and its impact, within organisations operating in the financial services sector in the UK and Ireland. They can be regarded as a benchmark of good practice against which organisations can assess their internal audit function.											
Who is it for? 2. The intended audience for this publication includes chief audit executives, executive and non-executive directors, and in particular members of audit and risk committees, working in the financial services sector and regulatory bodies. This Code contains provisions which are specific to the financial services sector. Internal audit functions outside the financial services sector and within the private and third sectors should follow the 'Internal Audit Code of Practice: Guidance on effective internal audit in the private and third sectors'. This Code may prove useful for internal audit in the public sector, but it is not drafted with the public sector specifically in mind, and public sector internal audit functions should continue to follow the Public Sector Internal Audit Standards.											
How should it be applied? 3. The Code of Practice should be applied in conjunction with the existing International Professional Practices Framework (IPPF) published by the global Institute of Internal Auditors, which includes the International Standards for the Professional Practice of Internal Auditing ('the IIA Standards'). The Code builds on those Standards, providing context specific to the financial services sector; and seeks to increase the effectiveness and impact of internal audit in organisations in that sector by clarifying expectations and requirements.											
How should it be applied? 4. The Code is principles-based. It is written in the context of a company operating within the UK and Ireland regulated financial services sector. It is expected that the procedural requirements of the Code should be applied proportionately, and therefore smaller organisations should apply the principles on which the Code is based and its procedural requirements in light of their size, risk profile and internal organisation and the nature, scope and complexity of their operations.											
[A] Role and mandate of internal audit											
5. The primary role of internal audit should be to help the board and executive management to protect the assets, reputation and sustainability of the organisation. It does this by assessing whether all significant risks are identified and appropriately reported by management and the risk function to the board and executive management; assessing whether they are adequately controlled; and by challenging executive management to improve the effectiveness of governance, risk management and internal controls. The role of internal audit should be articulated in an internal audit charter, which should be publicly available.											
6. The board, its committees and executive management should set the right 'tone at the top' to ensure support for, and acceptance of, internal audit at all levels of the organisation.											
[B] Scope and priorities of internal audit											
7. Internal audit's scope should be unrestricted. There should be no aspect of the organisation which internal audit should be restricted from looking at as it delivers on its mandate. Whilst it is not the role of internal audit to second guess the decisions made by the board and its committees, its scope should include information presented to the board and its committees as discussed further below.											
8. Risk assessments and prioritisation of internal audit work. In setting its scope, internal audit should form its own judgement on how best to segment the audit universe given the structure and risk profile of the organisation. It should take into account business strategy and should form an independent view of whether the key risks to the organisation have been identified, including emerging and systemic risks, and assess how effectively these risks are being managed. Internal audit's independent view should be informed, but not determined, by the views of management or the risk function. In setting out its priorities and deciding where to carry out more detailed work, internal audit should focus on the areas where it considers risks to be higher. Internal audit should make a risk-based decision as to which areas within its scope should be included in the audit plan – it does not necessarily have to cover all of the scope areas every year. Its judgement on which areas should be covered in the audit plan, and on the frequency and method of audit cycle coverage, should be subject to approval by the audit committee.											
9. Internal audit coverage and planning. Internal audit plans, and material changes to internal audit plans, should be approved by the audit committee. They should have the flexibility to deal with unplanned events to allow internal audit to prioritise emerging risks. Changes to the audit plan should be considered in light of internal audit's ongoing assessment of risk.											
10. Scope of internal audit. The scope of internal audit's work should be regularly reviewed to take account of new and emerging risks. Where relevant, internal audit should assess not only the process followed by the organisation's first and second lines, but also the quality of their work. As a minimum, internal audit should include within its scope the following areas											
a. Internal governance. Internal audit should include within its scope the design and operating effectiveness of the internal governance structures and processes of the organisation.											
b.The information presented to the board and executive management for strategic and operational decision making. Internal audit should include within its scope the processes and controls supporting strategic and operational decision making. It should assess whether the information presented to the board and executive management, fairly represents the benefits, risks and assumptions associated with the strategy and corresponding business model.											
c. The setting of, and adherence to, the risks the entity is willing to accept (risk appetite). Internal audit is not responsible for setting the risk appetite but should assess whether the risk appetite has been established and reviewed through the active involvement of the board and executive management. It should assess whether risk appetite is embedded within the activities, limits and reporting of the organisation; and it should report annually to the audit and risk committees its conclusions on whether the organisation's risk appetite framework is being adhered to.											
d. The risk and control culture of the organisation. Internal audit should include within its scope the risk and control culture of the organisation. This should include assessing whether the processes (e.g. appraisal and remuneration), actions (e.g. decision making), 'tone at the top' and observed behaviours across the organisation are in line with the espoused values, ethics, risk appetite and policies of the organisation. Internal audit should consider the attitude and assess the approach taken by all levels of management to risk management and internal control. This should include management's actions in addressing known control deficiencies as well as management's regular assessment of controls.											
e. Risks of poor customer treatment, giving rise to conduct or reputational risk. Internal audit should evaluate whether the organisation is acting with integrity in its dealings with customers and in its interaction with relevant markets. Internal audit should evaluate whether business and risk management is adequately designing and controlling products, services and supporting processes in line with customer interests, protection of customer data and conduct regulation.											
f. Capital and liquidity risks. Internal audit should include within its scope the modelling and management of the organisation's capital and liquidity risks, including the process for establishing and maintaining scenario analysis (stress testing) in relation to major risk categories, and recovery plans related to economic shocks.											
g. Key corporate events. Examples of key corporate events could include significant business process changes, introduction of new products and services, outsourcing decisions and acquisitions/ divestments. Internal audit should decide on a timely basis if these events are sufficiently high risk to warrant involvement. In doing so, internal audit will evaluate whether the key risks are being adequately addressed (including by other forms of assurance, e.g. due diligence) and reported. Internal audit should also assess whether the information being used in such key decision making is fair, balanced and reasonable, and whether the related procedures and controls have been followed.											
h. Outcomes of processes. Internal audit should evaluate the design and operating effectiveness of the organisation's policies and processes. In doing so, it should not adopt a 'tick box' approach based purely on the design of processes and controls, and should always consider the actual outcomes which result from their application, assessed against the espoused values, ethics, risk appetite and policies of the organisation.											
[C] Reporting results											
11. Internal audit should be present at, and issue reports to the appropriate governing bodies, including the board audit committee, the board risk committee and any other board committees as appropriate. The nature of the reports will depend on the remits of the respective governing bodies.											
12. Internal audit's reporting to the board audit, board risk and any other board committees should include:											
• a focus on significant control weaknesses and breakdowns together with a robust root-cause analysis. Internal audit's reports should identify owners, accountabilities and timescales for each management action;											

• any thematic issues identified across the organisation;											
• an independent view of management's reporting on the risk management of the organisation, including a view on management's remediation plans (which might include restricting further business until improvements have been implemented), highlighting areas where there are significant delays;											
• a review of any post-mortem and 'lessons learned' analysis if a significant adverse event has occurred at an organisation (for example, a regulatory breach). Any such review should assess both the role of the first and second lines and internal audit's own role; and											
• at least annually, an assessment of the overall effectiveness of the governance, and risk and control framework of the organisation, and its conclusions on whether the organisation's risk appetite framework is being adhered to, together with an											
[D] Interaction with risk management, compliance and finance											
13. Effective risk management, compliance and finance functions are an essential part of an organisation's corporate governance structure. Internal audit should be independent of these functions and be neither responsible for, nor part of, them.											
14. Internal audit should include within its scope an assessment of the adequacy and effectiveness of the risk management, compliance and finance functions. In evaluating the effectiveness of internal controls and risk management processes, in no circumstances should internal audit rely exclusively on the work of risk management, compliance or finance. Internal audit should always examine, for itself, an appropriate sample of the activities under review.											
15. Internal audit should exercise informed judgement as to what extent it is appropriate to take account of relevant work undertaken by others, such as risk management, compliance or finance in either its risk assessment or determination of the level of audit testing of the activities under review. Any judgement which results in less intense internal audit scrutiny should only be made after an evaluation of the effectiveness of that function in relation to the area under review.											
[E] Independence and authority of internal audit											
16. The chief audit executive should be at a senior enough level within the organisation (normally expected to be at executive committee or equivalent) to have the appropriate standing, access and authority to challenge the executive. Subsidiary, branch and divisional heads of internal audit should also be of a seniority comparable to the senior management whose activities they are responsible for auditing.											
17. Internal audit should have the right to attend and observe all or part of executive committee meetings and any other key management decision making fora. This enables internal audit to understand better the strategy of the business, key business issues and decisions, and to adjust internal audit priorities where appropriate. It also facilitates a better working relationship with executive committee members.											
18. Internal audit should have sufficient and timely access to key management information and a right of access to all of the organisation's records, necessary to discharge its responsibilities. In organisations in which the internal audit function is outsourced this Code still applies, and the chief audit executive should always be employed directly by the organisation to ensure they have sufficient and timely access to key management information and decisions.											
19. The primary reporting line for the chief audit executive should be to the chair of the audit committee.											
20. The audit committee should be responsible for appointing the chief audit executive and removing him/her from post.											
21. The chair of the audit committee should be accountable for setting the objectives of the chief audit executive and appraising his/her performance at least annually. It would be expected that the objectives and appraisal would take into account the views of the chief executive. This appraisal should consider the independence, objectivity and tenure of the chief audit executive. Where the tenure of the chief audit executive exceeds seven years, the audit committee should explicitly discuss annually the chair's assessment of the chief audit executive's independence and objectivity.											
22. The chair of the audit committee should be responsible for recommending the remuneration of the chief audit executive to the remuneration committee. The remuneration of the chief audit executive and internal audit staff should be structured in a manner that avoids conflicts of interest, does not impair their independence and objectivity and should not be directly or exclusively linked to the short term performance of the organisation.											
23. Subsidiary (including ring-fenced bank), branch and divisional heads of internal audit should report primarily to the Group chief audit executive, while recognising local legislation or regulation as appropriate. This includes the responsibility for setting budgets and remuneration, conducting appraisals and reviewing the audit plan. The Group chief audit executive should consider the independence, objectivity and tenure of the subsidiary, branch or divisional heads of internal audit when performing their appraisals.											
24. If internal audit has a secondary executive reporting line, this should be to the CEO in order to preserve independence from any particular business area or function and to establish the standing of internal audit alongside the executive committee members.											
[F] Resources											
25. The chief audit executive should ensure that the audit team has the skills and experience, including technical subject matter expertise, commensurate with the scale of operations and risks of the organisation. This may entail training, recruitment, secondment from other parts of the organisation or co-sourcing with external third parties.											
26. The chief audit executive should provide the audit committee with a regular assessment of the skills required to conduct the work needed, and whether the internal audit budget is sufficient to recruit and retain staff or procure other resources with the expertise, experience and objectivity necessary to provide effective challenge throughout the organisation and to the executive.											
27. The audit committee should be responsible for approving the internal audit budget and, as part of the board's overall governance responsibility, should disclose in the annual report whether it is satisfied that internal audit has the appropriate resources.											