Chartered Institute of Internal Auditors

20 April 2020

Financial services code

Chartered Institute of Internal Auditors

Effective internal audit in the financial services sector

This code, published in July 2013, was produced by an independent committee established by the IIA, with representation and observers from leading banks, insurers, the Financial Conduct Authority, the Prudential Regulation Authority and the Bank of England.

The code was reviewed and published in September 2017 with only modest changes.

Read on to view the code and further guidance.

Context

The recommendations which follow are aimed at enhancing the overall effectiveness of Internal Audit, and its impact, within the firms operating in the financial services sector in the UK. They can be regarded as a benchmark of good practice against which firms can assess their Internal Audit function. The intended audience for this publication includes Chief Internal Auditors, executive and non-executive directors, and in particular members of Audit and Risk Committees, and regulatory bodies.

The recommendations should be applied in conjunction with the existing International Professional Practices Framework published by the global Institute of Internal Auditors, which includes the International Standards for the Professional Practice of Internal Auditing ('the IIA Standards'). They build on those Standards, providing Context context specific to the financial services sector; and seeking to increase the effectiveness and impact of Internal Audit in organisations in that sector by clarifying expectations and requirements.

The recommendations are principles-based, rather than establishing detailed rules. They are written in the context of a reasonably-sized company operating within the UK regulated financial services sector. Small companies and branches of non-UK headquartered organisations in particular might need to make some modifications to the detail, in the light of their size, risk profile and internal organisation, and the nature, scope and complexity of their operations: but all should comply with the principles.

Role and mandate of internal audit

1. 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.

2. 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.

Scope and priorities of internal audit

3. 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.

4. 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.

5. 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. The changes, to the audit plan should be considered in light of Internal Audit's ongoing assessment of risk.

6. 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 of defence, 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, 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 Committee 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 are adequately designing and controlling products, services and supporting processes in line with customer interests 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.

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 if these events are sufficiently high risk to warrant involvement on a real time basis. In doing so, Internal Audit will evaluate whether the key risks are being adequately addressed (including by other forms of assurance, e.g. third party 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 andpolicies of the organisation.

Reporting results

7. 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.

8. Internal Audit's reporting to the Board Audit and/or Risk 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 of defence 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 analysis of themes and trends emerging from Internal Audit work and their impact on the organisation's risk profile.

Interaction with risk management, compliance and finance

9. 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.

10. 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.

11. 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.

Independence and authority of internal audit

12. The Chief Internal Auditor should be at a senior enough level within the organisation (normally expected to be at Executive Committee or equivalent) to give him or her 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.

13. 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.

14. 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, the Chair of the Audit Committee should identify an appropriate individual responsible for ensuring that the Chief Internal Auditor has sufficient and timely access to key management information and decisions.

15. The primary reporting line for the Chief Internal Auditor should be to the Chair of the Audit Committee. In exceptional circumstances, the Board may wish for Internal Audit to report directly to the Chair of the Board, or delegate responsibility for the reporting line to the Chair of the Board Risk Committee, provided the Chair of the Board Risk Committee and all the other Committee members are independent Non-Executive Directors. The reporting line must avoid any impairment to Internal Audit's independence and objectivity.

16. The Audit Committee should be responsible for appointing the Chief Internal Auditor and removing him/her from post.

17. The Chair of the Audit Committee should be accountable for setting the objectives of the Chief Internal Auditor 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 Internal Auditor. Where the tenure of the Chief Internal Auditor exceeds seven years, the Audit Committee should explicitly discuss annually the Chair's assessment of the Chief Internal Auditor's independence and objectivity.

18. The Chair of the Audit Committee should be responsible for recommending the remuneration of the Chief Internal Auditor to the Remuneration Committee. The remuneration of the Chief Internal Auditor and Internal Audit staff should be structured in a manner such that it 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.

19. Subsidiary (including ring-fenced bank), branch and divisional Heads of Internal Audit should report primarily to the Group Chief Internal Auditor, 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 Internal Auditor should consider the independence, objectivity and tenure of the subsidiary, branch or divisional Heads of Internal Audit when performing their appraisals.

20. 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.

Resources

21. The Chief Internal Auditor 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.

22. The Chief Internal Auditor 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.

23. 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.

Quality assessment

24. The Board or the Audit Committee is responsible for evaluating the performance of the Internal Audit function on a regular basis. In doing so it will need to identify appropriate criteria for defining the success of Internal Audit. Delivery of the audit plan should not be the sole criterion in this evaluation.

25. Internal Audit should maintain an up-to-date set of policies and procedures, and performance and effectiveness measures for the Internal Audit function. Internal Audit should continuously improve these in light of industry developments.

26. Internal Audit functions of sufficient size should develop a quality assurance capability, with the work performed by individuals who are independent of the delivery of the audit. The individuals performing the assessments should have the standing and experience to meaningfully challenge Internal Audit performance and to ensure that Internal Audit judgements and opinions are adequately evidenced.

The scope of the quality assurance review should include Internal Audit's understanding and identification of risk and control issues, in addition to the adherence to audit methodology and procedures. This may require the use of resource from external parties. The quality assurance work should be risk-based to cover the higher risks of the organisation and of the audit process. The results of these assessments should be presented directly to the Audit Committee at least annually.

27. Where the Internal Audit function is outsourced to an external provider, Internal Audit's work should be subject to the same quality assurance work as the in-house functions. The results of this quality assurance work should be presented to the Audit Committee at least annually for review.

28. In addition, the Audit Committee should obtain an independent and objective external assessment at appropriate intervals, irrespective of the size of the organisation. This could take the form of periodic reviews of elements of the function, or a single review of the overall function. In any event, the Internal Audit function as a whole should as a minimum be subject to a review at least every five years, as set out in the International Professional Practice Framework for Internal Audit. The conformity of Internal Audit with this guidance should be explicitly included in this evaluation. The Chair of the Audit Committee should oversee and approve the appointment process for the independent assessor.

Relationships with regulators

29. Nature and purpose of the relationship

The Chief Internal Auditor, and other senior managers within Internal Audit, should have an open, constructive and co-operative relationship with regulators which supports sharing of information relevant to carrying out their respective responsibilities.

Wider considerations

30. The Chartered Institute of Internal Auditors should develop practical materials for Internal Auditors on the application and implementation of specific aspects of this guidance, aimed in particular at
smaller institutions. Such material should focus on examples of good practice, and should not be seen as adding to the requirements of this guidance. In particular, less well established areas for Internal Audit activity would benefit from such material.

31. The Chartered Institute of Internal Auditors should commission further independent reviews of this guidance every five years, in the light of further experience, with a view to deciding whether any further changes are required.

Associated guidance

This series of guidance pulls together further information and resources to help you implement the revised financial services code.

Annual governance, risk and control assessments
This guidance sets out a framework to enable the internal audit practitioner to fulfil requirements under paragraph 8 and 6c of the revised Code.

Auditing new product development
Understand how to audit new products and provide assurance that new risks are being mitigated.

Bank's capital and liquidity – auditing ICAAP and ILAAP
Assessing both the governance and adequacy of your organisations ICAAP and ILAAP are discussed in this piece of guidance.

Internal audit effectiveness
How to ensure that your internal audit function is effective and meeting the requirements under the FS Code and IIA Standards.

Outcomes of processes
One method to test the outcomes, rather than outputs, of processes.

Retrospective reviews
What are adverse events, and what should internal audit be doing?

Risk assessments and prioritisation of internal audit work
Methods to segment the audit universe and provide assurance to your audit committee that your team is covering all critical issues.

Further reading

Comparison between the FS code and the International Standards

The Chartered Institute of Internal Auditors and IIA Global have jointly produced a comparative guide, outlining the relationship between the Financial Services Code and the International Standards. This is presented in two ways:

Effective Internal Audit in the Financial Services Sector - The Standards mapped to the recommendations
Effective Internal Audit in the Financial Services Sector - The recommendations mapped to the Standards

Research and insight

Implementing the IIA Financial Services Code - Surfing the wave - 2015 review of how internal audit functions in financial services institutions have changed since the introduction of the our Financial Services Code in 2013.

Building effective internal audit - In this report, we look at how firms in the UK financial services sector are successfully implementing the individual recommendations contained within the IIA's

Financial Services Code Effective Internal Audit in the Financial Services Sector. These examples of good practice are also relevant for increasing the effectiveness of internal audit in other sectors.

Embedding effective internal audit in the financial services sector - A survey of heads of internal audit to find out what progress they were making on implementing the IIA's financial services code from 2014.

Other policy initiatives

Details of the evolving story of the code and other policy initiatives are in the Policy and Research section.

Audio & video

Thanks to EY for permission to use their audio/visual material.

Follow this link to view the video

Can't see the video above? Then watch it on YouTube.

Listen to the complete audio track from the video.