National Audit Office

REPORT

Bank of England: Managing legal, ethical and staff compliance risks

Bank of England

SESSION 2023-24
4 MARCH 2024
HC 578

Key facts

2017

the year the Bank of England (the Bank) began making major changes to how it manages non-financial risks (risks to the Bank's operations or reputation that would not directly affect its balance sheet)

19

the number of key types of non-financial risks the Bank has identified, of which our report has focused on four compliance risks (legal; conflicts of interest and business ethics; compliance; and procurement)

5 to 10

number of 'critical metrics' the Bank uses to monitor each key type of compliance risk and inform decisions on whether action is needed

The Bank has acted to promote and embed a culture of risk awareness and speaking up, but recognises it has more to do:

1,400 approximate number of staff as at February 2023 (around a quarter of the Bank's headcount) who had been at the Bank less than two years, which creates challenges and opportunities for embedding a risk awareness culture

59% proportion of staff the Bank surveyed in 2023 who felt they were free to speak their mind without fear of negative consequences

The Bank is working to clarify and, where appropriate, simplify staff policies and related controls:

78 number of internal policies that staff across the Bank should comply with in 2023, which it reduced from 393 in 2020 to make it easier for staff to understand their responsibilities

465 number of separate controls (actions, tools and processes intended to reduce the likelihood or impact of a risk) the Bank's Compliance division has documented in relation to its key policies and standards

The Bank has updated its systems to make risk assessment and management more consistent:

39 number of separate risk registers that the Bank replaced with a single risk management information system in January 2023

Summary

1 The Bank of England (the Bank) is the UK's central bank. Its core mission is to promote the good of the people of the UK by maintaining monetary and financial stability. It has a range of roles that include: setting monetary policy; setting policy for financial stability; producing bank notes; supporting financial markets and the settlement of transactions; and regulating the stability of financial institutions (since 2013). The Bank is operationally independent of government and accountable to Parliament and the public.

2 The Bank relies on public trust and its reputation for integrity to carry out its role. On the webpage for its code of conduct, the Bank says it is "committed to promoting the highest standards of integrity and high ethical standards within the organisation" to maintain the public trust it relies on to achieve its aims. The Bank seeks to ensure it complies with legal and ethical requirements, and it publishes its staff code of conduct setting out the key conduct policies its people should follow. Its staff policies cover matters such as conflicts of interest, data protection, use of Bank resources, and safety and security.

3 Past incidents at the Bank and in other public bodies have shown how failure to demonstrate integrity can harm an organisation's credibility and reputation. For example, in 2017 one of the Bank's deputy governors resigned after failing to formally declare to the Bank a senior level conflict of interest within the banking industry. Similarly, in 2019, the Bank established that procurement and technology weaknesses had not detected a third-party supplier intentionally streaming press conferences with market-sensitive information more quickly than other sources, giving its subscribers a potential market advantage. The Bank commissioned full reviews of those incidents, including how it manages conflicts of interest. Since 2017, it has also developed a new, more substantive overall approach to managing non-financial risks, which are risks to the Bank's operations or reputation that would not directly affect its balance sheet.

Scope of the report

4 This report examines whether the Bank has efficient and effective systems and processes to manage risks of non-compliance with legal, ethical and staff policy requirements (referred to as 'compliance risks' in the rest of this report). Within these areas, this report focuses on compliance risks relating to how the Bank functions as an organisation that could affect its credibility and effectiveness if not managed well.

5 The report covers:

- the Bank's overall approach to managing compliance risks, and how it has developed this since 2017 (Part One);
- whether the Bank has the processes and information it needs to identify, assess and monitor compliance risks effectively (Part Two); and
- whether the Bank responds to compliance risks in a way that supports timely and effective decisions, and uses lessons to improve its approach (Part Three).

6 Our remit to audit the Bank does not cover certain areas of its work, such as its supervision of the banking sector and the decisions of its policy committees. We have assessed the systems and processes informing risk management decisions, but have not assessed the merits of individual decisions themselves (for example, on setting risk tolerance or responding to individual incidents).

7 We have not sought to evaluate the Bank's overall risk management framework or how successfully the Bank is mitigating risks, but we have assessed how the framework is designed and operates in relation to the compliance risk areas our study covers. We also did not examine in detail every compliance risk the Bank faces. We supplemented our assessment of its overall approach with a sample of specific risk areas that we examined in more depth. These were: conflicts of interest; internal whistleblowing; data protection and privacy; compliance with procurement law; and avoiding inappropriate use of resources through procurement processes. Examples within our report are intended to illustrate our findings and not generalise across the Bank's overall approach to risk management.

Key findings

How the Bank manages compliance risks

8 The Bank's overall framework for managing non-financial risks, including compliance risks, contains the main features we expect to see. While an effective risk management framework will depend on the specific risks an organisation faces, there are several key features we typically expect to see. These include: clear accountabilities and governance; processes that support identification, measurement and management of risks; a clear definition of what level of risk can be accepted; and regular risk assessment and monitoring of key risk indicators. Following reviews in 2017 and 2018, the Bank designed a new approach that it has continued to develop, and which we found contains these features. It created a dedicated Risk Directorate, under an executive director responsible for risk oversight and challenge. It also set clear lines of reporting and accountability, and consistent definitions and terminology to help staff understand and assess risks. Specific processes and information systems we reviewed were consistent with risk management practice we have seen in other organisations (paragraphs 1.6 to 1.9).

9 The Bank has acted to promote and embed a risk awareness culture, but recognises it has more to do. To operate well in practice, a risk management framework requires a good culture of risk awareness that supports staff to understand their responsibilities, identify risks and respond in a timely way. The Bank has highlighted the importance of risk culture in key internal documents and communications, including its overall risk management framework and annual code of conduct return required of all staff. In 2021, the Bank assessed its culture through interviews and a staff survey on speaking up. It found that there was not a clear message on its risk culture, and 51% of survey respondents felt that any concerns they raised would be addressed. This compares with 76% in central government bodies who answered a similar question in the 2021 Civil Service People Survey. In response, the Bank expanded its provision of training and workshops on risk awareness and speaking up, which it also adapted in response to a large number of new starters (approximately 1,400 staff as at February 2023 – around a quarter of the Bank's headcount – had been there less than two years). The Bank's Compliance team told us it also aimed to take a proportionate response to breaches, to create a healthy and open culture where staff are more likely to report incidents or concerns. However, it will take time to fully embed this culture, and the Bank recognises it has more to do. It has included new questions in its annual staff survey to monitor progress, which in 2023 found that 59% of staff surveyed felt they were free to speak their mind without fear of negative consequences (paragraphs 1.20 to 1.26).

10 The Bank has made good progress since 2017 in developing how it manages compliance risks, and is planning further improvements. It has externally benchmarked its approach in specific areas through engaging with similar organisations and by commissioning the Institute of Business Ethics to review its code of conduct. It also reduced the number of internal policies staff should comply with from 393 in 2020 to 78 in 2023, to make it easier for people to understand their responsibilities. The Bank told us that, while it is confident it has robust processes to manage legal risks, there is more to do to manage wider compliance risks effectively, and it plans further work to continue improving its approach. For example, its planned work for 2024-25 includes improvements to the quality and consistency of information recorded in risk registers, linking risk management activities to business plans and budgets, and a more consistent process for responding to incidents once they have been reported. The Bank's Compliance team also plans to further develop how it engages with and supports other parts of the Bank to ensure staff policies are understood and followed (paragraphs 1.21 and 1.28 to 1.30).

Identifying, assessing and monitoring risks

11 The Bank makes good use of internal and external expertise to identify new or changing compliance risks and share good practice. Each of the Bank's 19 key non-financial risk types is overseen by a 'risk custodian' with relevant expertise. For example, officials across the Bank are responsible for managing legal risks in their business areas, but the Bank's General Counsel is the overall custodian for legal risks. These custodians work with other parts of the Bank and counterparts in other organisations to identify new or changing compliance risks and provide updates to the Bank's quarterly horizon-scanning exercise. The Bank's Risk Directorate reviews and challenges these updates alongside its own Bank-wide analysis. It then reports quarterly to the relevant risk committees, primarily its Executive Risk Committee and the non-executive Audit and Risk Committee, to provide information and, where relevant, inform decision-making (paragraphs 2.4 to 2.7).

12 The Bank's business areas regularly assess compliance risks using a consistent approach, but do not always explain changes in a risk's likelihood or impact. 'Risk and control self-assessment' is a common risk management process for identifying and assessing operational risks and the adequacy of controls in place. The Bank uses this process when a risk is added to the risk register and then quarterly, requiring business areas to update their assessment of each risk. In January 2023, the Bank replaced 39 separate risk registers with a single information system. This system records assessments in a consistent format the Risk Directorate can scrutinise, challenge where necessary, and consolidate into a Bank-wide assessment. We found that the information required was aligned with standard practice, including quantifying each risk's likelihood and impact with and without controls, and commentary on the assessment including the adequacy of the controls. In the compliance risk areas we examined, we found that business areas regularly updated the system on a consistent basis, but there was variation in the level of detail provided to explain assessments. In some cases, business areas changed their assessed level of risk since the previous quarter but did not explain the cause or impact of the change (paragraphs 2.2, 2.3 and 2.9 to 2.13).

13 The Bank has developed a clear set of relevant key metrics for each type of compliance risk, which it monitors and reports regularly to decision-makers. Effective risk monitoring allows organisations to understand where risks are outside of acceptable levels and when action may be required. For each key risk type, the Bank has introduced a set of five to 10 quantified 'critical metrics'. For example, the critical metrics for business ethics and conflicts of interest include numbers of major breaches (such as senior level conflicts that materially affect an official's independence but have not been disclosed) and minor breaches (such as retrospective approvals for personal financial transactions that should have been approved in advance). Risk custodians for each risk type work with the Risk Directorate to agree a set of critical metrics and provide updated figures each quarter. The Risk Directorate collates these metrics and reports them quarterly alongside its Bank-wide assessment of 'amber'- and 'red'-rated risks to the Executive Risk Committee and Audit and Risk Committee (paragraphs 2.14 to 2.19).

14 The Bank has established a consistent process for quantifying its appetite and tolerance for each compliance risk and the metrics it uses to monitor them. To decide whether action is needed, organisations need to clearly define the level of risk they can accept, against which their assessment and monitoring can be compared. The Bank's overall approach to compliance risks is a very low tolerance for deliberate breaches (including zero tolerance for deliberate breaches of laws and regulations) and a proportionate response to other breaches based on the potential impact on the Bank's credibility and effectiveness. The Bank uses a consistent framework and criteria for assessing whether each risk should be rated 'red', 'amber' or 'green' based on its likelihood and impact. Business areas also set a target rating for each risk and, where relevant, a target date to reach it. Risk custodians work with the Risk Directorate to agree quantified thresholds for each critical metric, which are ultimately agreed by the Audit and Risk Committee. Setting these is a matter of judgement, and we did not review the rationale for individual risks or metrics. In the areas we examined, we found that critical metrics' thresholds were well aligned to the Bank's overall approach (paragraphs 2.20 to 2.22).

Responding to risks effectively

15 The Bank does not yet test the operating effectiveness of all its key controls to manage compliance risks, and plans to implement a more consistent approach. Controls are actions, tools and processes intended to reduce the likelihood of a risk materialising or the impact it would have if it materialised. For each risk, the Bank documents the relevant controls and an assessment of their adequacy. The Bank has not conducted an assurance mapping exercise to identify whether its controls are sufficiently complete, or whether there are gaps or duplication. However, its Compliance team has worked with other parts of the Bank to identify 465 risk management controls for its key policies and standards and is working to reduce duplicates. The Risk Directorate has similarly begun work to identify controls that cut across different risks and business areas. It also recently introduced functionality to its systems to document evidence and testing of whether controls are working effectively. The Bank told us that, while some areas such as the Legal Directorate already test the operating effectiveness of their controls, outside the Legal Directorate there are some key controls for which there is not yet evidence of such testing. Its plans for 2024-25 include implementing a risk-based approach to prioritise controls for testing (paragraphs 3.2 to 3.9).

16 Minor compliance breaches of staff policies have been above a level the Bank considers acceptable, and it has set action plans aimed at reducing them. For the compliance risks in the scope of our study, a small number of the Bank's critical metrics have consistently shown levels of minor compliance breaches higher than the thresholds it set. For example, this includes emails being sent to the wrong address, and late disclosures or retrospective approvals relating to conflicts of interest policies. The Bank told us that the vast majority of breaches are self-reported by Bank staff. In total there were 628 minor and 28 major compliance breaches in the year to August 2023. The Bank expects risk custodians to develop and implement specific action plans to bring critical metrics back within acceptable levels. Different parts of the Bank work together to implement these plans, including the Compliance team, risk custodians and business areas. While the Bank has taken steps to ensure it is clear what each action plan involves and who is responsible, the latest plans are new, and their impact is not yet known. For minor compliance breaches, the metrics had been outside thresholds for more than a year (paragraphs 3.11 to 3.13).

17 The Bank regularly acts to learn and implement lessons from breaches or near misses, though it does not routinely evaluate how well changes it makes are working. High-profile incidents in 2017 and 2019 prompted the Bank to conduct formal reviews of these incidents, identify lessons and ultimately overhaul its approach to managing non-financial risks. Since then, the Bank has continued to use less significant breaches and near misses to inform its approach to compliance risks. For example, the Bank has an 'incident review forum' to analyse its incident management system for root causes and lessons to learn, and to set plans to minimise re-occurrence. The Bank uses its risk monitoring to consider the overall effectiveness of its approach, and it has conducted some recent evaluations and benchmarking exercises. However, when it makes changes to risk and compliance arrangements, it does not set an expectation that these changes be formally evaluated (paragraphs 3.15 to 3.20).

Conclusion

18 Following high-profile incidents in 2017 and 2019, the Bank overhauled its approach to identifying and managing non-financial risks. It has made good progress in developing new and improved systems and processes to understand the risks it faces of non-compliance with legal and ethical requirements and staff policies, and to manage these in a responsive and proportionate way. This includes a clear set of relevant metrics to monitor how risks are changing over time, which it reports regularly to appropriate decision-makers, and a range of actions to improve risk awareness and understanding among staff.

19 However, the Bank recognises that it has more to do to ensure its systems and processes for managing compliance risks are effective in practice, and it is planning further improvements. As it takes forward its work in this area, the Bank should ensure it continues to improve the quality and consistency of the information it records on risk assessment and monitoring, and the awareness and confidence of staff to flag risks or highlight concerns.

Recommendations

20 The Bank has committed to continue enhancing how it manages compliance risks and has set plans in several areas. These recommendations are intended to help it in this process. The Bank should:

a Review whether there are material differences in awareness, understanding and perception of risk and compliance between different groups of staff – for example, based on role, seniority or length of service – in order to identify ways to target further improvements.

b Work with business areas to encourage them to more consistently explain changes in assessed levels of risk through the risk and control self-assessment process.

c Examine the completeness of the controls in place to manage compliance risks and whether there are gaps or duplication. This should cover: the areas on which the Bank requires assurance; the teams or control activities that provide assurance over each area; and the level of assurance provided by each team or activity. The Bank should identify the most cost-effective way to do this, including considering the merits of a formal assurance mapping exercise and any areas where it judges it already has robust assurance.

d Develop a programme of work to more regularly evaluate how well changes to risk management processes and policies are working in practice, and to understand the impact those changes have had on the Bank's ability to manage compliance risks effectively.