



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



We are the UK's independent public spending watchdog.

We support Parliament in holding government to account and we help improve public services through our high-quality audits.

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services.

The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent.

In 2022, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £572 million.



National Audit Office

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

Bank of England

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 29 February 2024

This report has been prepared under Section 6 of the
National Audit Act 1983 for presentation to the House of
Commons in accordance with Section 9 of the Act

Gareth Davies
Comptroller and Auditor General
National Audit Office

26 February 2024

Value for money reports

Our value for money reports examine government expenditure in order to form a judgement on whether value for money has been achieved. We also make recommendations to public bodies on how to improve public services.

The material featured in this document is subject to National Audit Office (NAO) copyright. The material may be copied or reproduced for non-commercial purposes only, namely reproduction for research, private study or for limited internal circulation within an organisation for the purpose of review.

Copying for non-commercial purposes is subject to the material being accompanied by a sufficient acknowledgement, reproduced accurately, and not being used in a misleading context. To reproduce NAO copyright material for any other use, you must contact copyright@nao.org.uk. Please tell us who you are, the organisation you represent (if any) and how and why you wish to use our material. Please include your full contact details: name, address, telephone number and email.

Please note that the material featured in this document may not be reproduced for commercial gain without the NAO's express and direct permission and that the NAO reserves its right to pursue copyright infringement proceedings against individuals or companies who reproduce material for commercial gain without our permission.

Links to external websites were valid at the time of publication of this report. The National Audit Office is not responsible for the future validity of the links.



Contents

Key facts 4

Summary 5

Part One

How the Bank manages
compliance risks 12

Part Two

Identifying, assessing and
monitoring risks 23

Part Three

Responding to risks effectively 31

Appendix One

Our audit approach 37

This report can be found on the National Audit Office website at www.nao.org.uk


If you need a version of this report in an alternative format for accessibility reasons, or any of the figures in a different format, contact the NAO at enquiries@nao.org.uk


The National Audit Office study team consisted of:


William Johnson,
Rich Sullivan-Jones,
Alberto Vanzo, Saniya Shah, with assistance from Tom Bowden and John Hemsley, under the direction of Simon Reason.

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157-197 Buckingham Palace Road
Victoria
London
SW1W 9SP

 020 7798 7400

 www.nao.org.uk

 @NAOorguk

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.

Part One

How the Bank manages compliance risks

1.1 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.

1.2 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.

1.3 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.¹ 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.

¹ Having disclosed it separately to the Treasury Select Committee in Parliament.

1.4 This Part sets out the Bank's overall approach to managing risks of non-compliance with legal, ethical and staff policy requirements (referred to as 'compliance risks' in the rest of this report). It covers:

- how the Bank has changed its approach since 2017;
- the Bank's overall framework for managing compliance risks and whether this includes the features we expect to see;
- what progress the Bank has made in promoting a risk awareness culture among its staff; and
- how the Bank seeks to continually improve and update its approach.

Changes since 2017

1.5 In 2017, the Bank's board of directors (known as the 'Court') reviewed how the Bank managed conflicts of interest, which included recommendations regarding its wider approach to managing compliance risks. In response, in 2018, the Bank reviewed how it allocated executive responsibility and organisational structures for managing risk.

1.6 Following these reviews, the Bank created a dedicated Risk Directorate, led by a new executive director role responsible for risk oversight and challenge across the Bank. This directorate brought together the divisions previously responsible for financial and non-financial risk, as well as the Bank's Compliance division. The Compliance division works to ensure staff comply with internal policies, and previously reported to the Bank's Secretary. The Bank also made changes to the seniority of certain roles or lines of reporting to strengthen its risk governance.

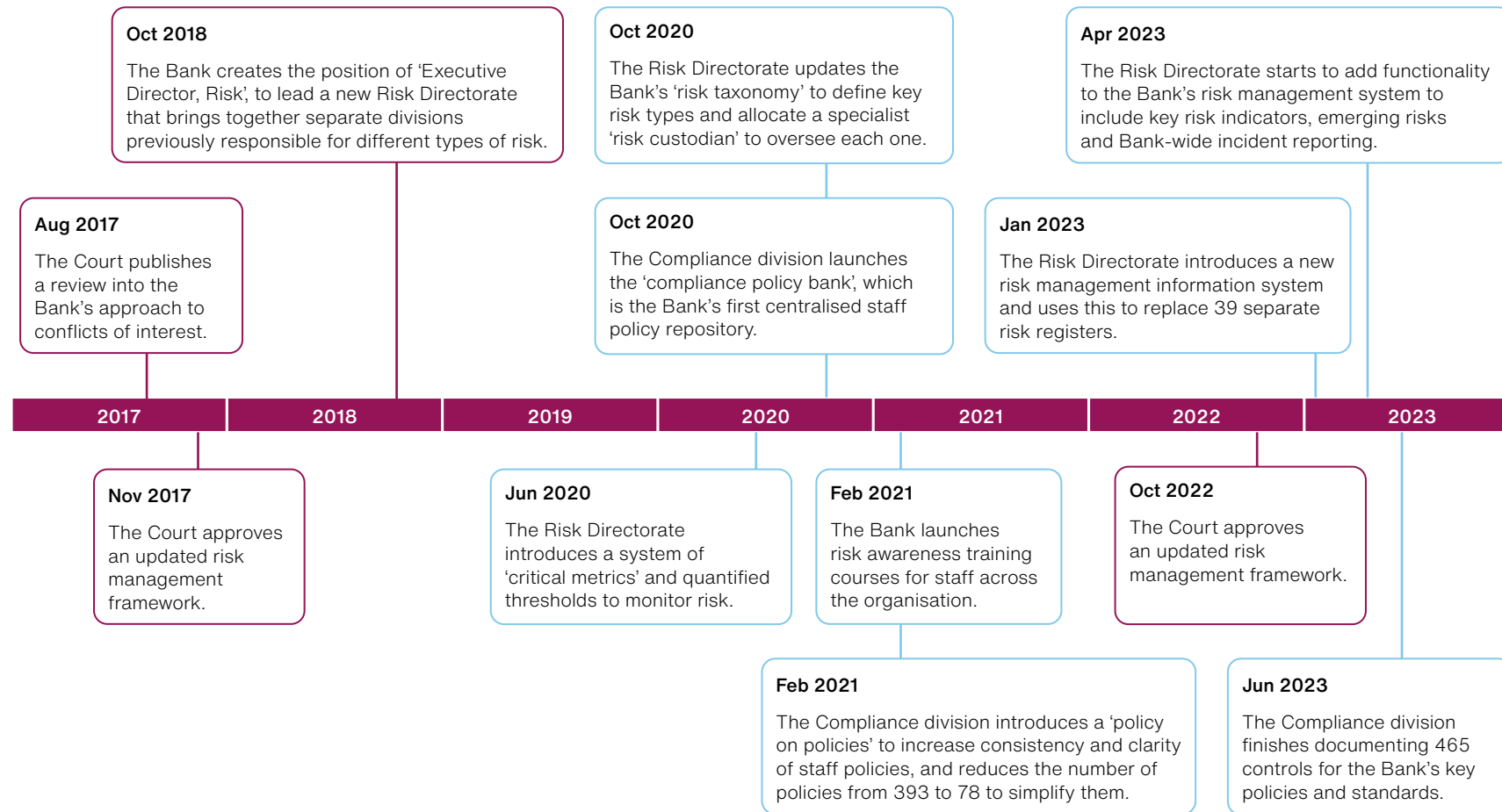
1.7 Since 2018, the Bank has continued updating its approach to managing compliance and other non-financial risks (**Figure 1** overleaf). Examples include:

- an updated overall risk management framework, which the Court most recently approved in 2022;
- a new, commercially available, risk management information system that replaced 39 separate manual risk registers and other risk information;
- updated definitions and categorisation of risks to ensure they are clear and comprehensive, including 19 key types of non-financial risk – each key risk type is overseen by a senior level 'risk custodian' with relevant expertise; and
- a new set of quantified 'critical metrics' for each key risk type, and more clearly defined thresholds to monitor whether each metric is at a level the Bank can accept – we examine critical metrics and relevant thresholds in Part Two.

Figure 1

Timeline of key changes to the Bank of England's (the Bank's) risk management approach since 2017

Since 2017, the Bank has made major changes to how it manages non-financial risks



□ Approvals by the Court
 □ Initiatives taken by the Bank's Risk Directorate

Notes

- 1 The Court is the Bank's board of directors.
- 2 Non-financial risks are risks to the Bank's operations or reputation that would not directly affect its balance sheet.

Source: National Audit Office review of Bank of England documentation

Design of the Bank's risk management framework

1.8 While an effective risk 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 for identifying and managing risks, including at senior levels;
- processes that support identification, measurement, and management of risks;
- a clear definition of what level of risk can be accepted, overall and in specific areas;
- a consistent and appropriately detailed approach to regularly assessing risk across the organisation; and
- regular monitoring and reporting of key risk indicators to inform decisions on whether action is needed.

1.9 We reviewed the Bank's overall framework for managing compliance and other non-financial risks and found that it contains the main features we expect to see. The changes the Bank has introduced since 2017 have brought its risk management framework design in line with good practice. Specific processes and information systems we reviewed were consistent with risk management practice we have seen in other organisations.

1.10 This section explains the main features of the Bank's current approach to managing compliance risks. The rest of Part One then examines the Bank's work to improve how its approach operates in practice. We assess specific parts of the Bank's approach in Part Two and Part Three.

The Bank's overall risk management framework

1.11 The Bank manages risks through an overarching risk management framework. The Bank aims to ensure consistency and transparency in risk management across the organisation, and to support a risk awareness culture where all staff share responsibility for effective risk management. The Bank's Court of directors aims to formally review the framework at least once every three years, and most recently approved it in October 2022.

1.12 The Bank's risk management framework establishes risk governance arrangements, processes for identifying, assessing and monitoring risks, and how to categorise risks.

Governance

1.13 The Bank's risk governance sits at both executive and non-executive levels (**Figure 2** on pages 17 and 18). The Court of directors is ultimately responsible for approving the risk management framework and setting the Bank's risk tolerance. It also has a lead role in setting a risk management culture, and reviews performance by setting the work programme of the Independent Evaluation Office, which provides reports to the Chair of the Court.

1.14 The Audit and Risk Committee (ARCo) is a sub-committee of Court responsible for reviewing, and reporting to Court on, the effectiveness of the Bank's risk management framework and internal control systems. ARCo reviews quarterly risk updates from the Bank's Risk Directorate, and considers whether the Bank can meet its objectives in light of these updates.

1.15 The Executive Risk Committee (ERC) is the main forum for executive oversight and challenge of how the Bank is managing key risks and whether it is consistent with the risk tolerance the Court approves. ERC sets the Bank's priorities for actions and resources to address key risks, commissions 'deep dive' reviews into specific areas, and reviews quarterly risk updates from the Risk Directorate.

Risk management processes

1.16 The Bank uses a 'three lines of defence' model to distinguish between those responsible for owning and managing risks, those responsible for providing oversight, support and challenge across the Bank, and those responsible for providing assurance (**Figure 3** on page 18). This is a standard approach widely used in risk management. For example, the Bank contributed to a benchmarking exercise with central banks in other countries, which found that most respondents (96%) used this model.

1.17 The Bank's risk management framework sets out four key stages for managing risks:

- Identifying new or changing risks through a range of methods and sources, including a quarterly horizon-scanning exercise and risk assessment process.
- Assessing the scale of risks and adequacy of controls in managing them, and monitoring critical metrics for key risk types.
- Implementing actions to address risks and ensure they remain in, or return to, acceptable levels set by Court.
- Reporting risk assessment and monitoring updates to executive and non-executive decision-makers. The Risk Directorate provides updates at least quarterly to ERC and ARCo, and twice a year to Court.

Figure 2

Governance of non-financial risks at the Bank of England (the Bank), 2023

Several areas of the Bank are responsible for managing and monitoring compliance risks

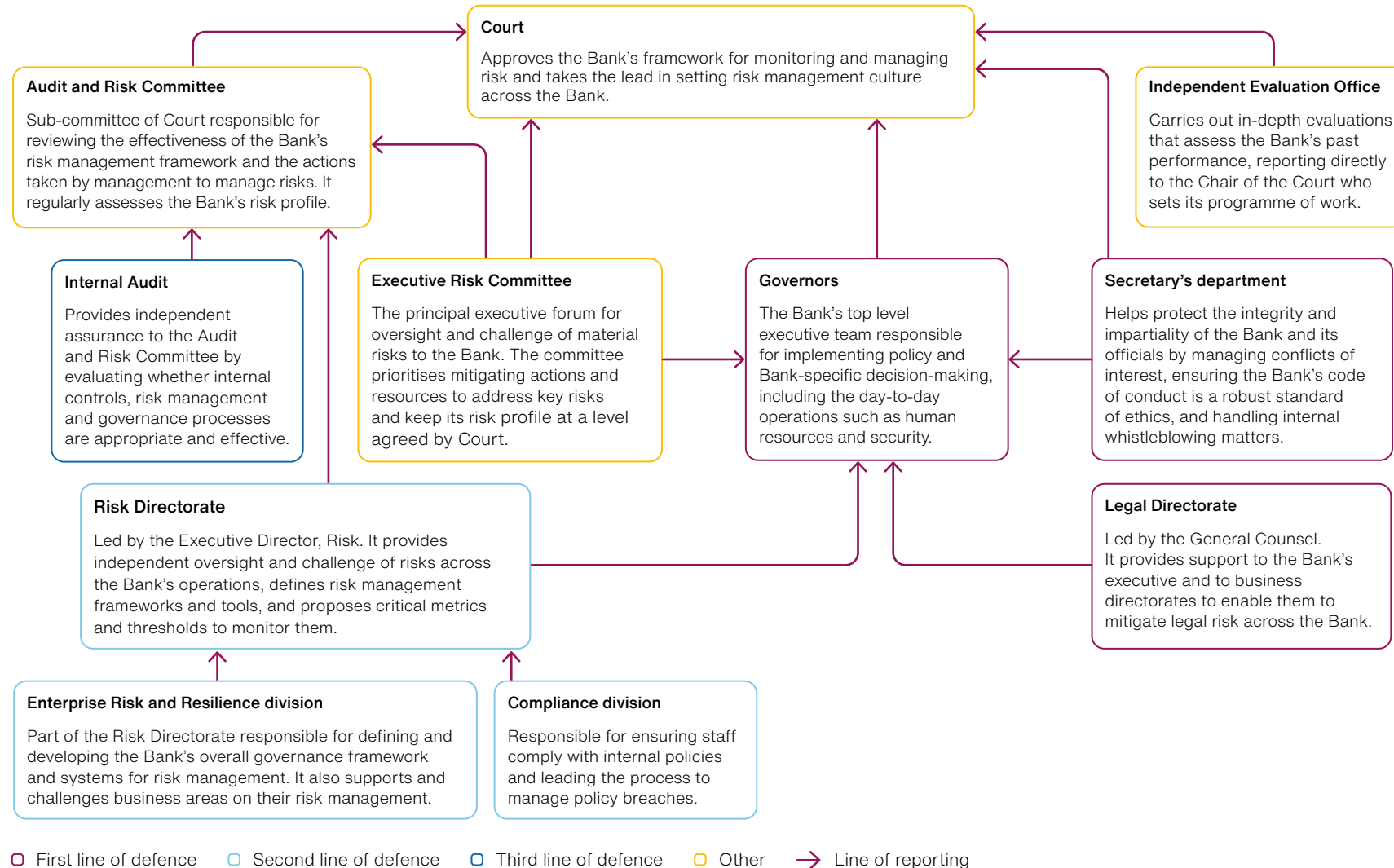


Figure 2 *continued*

Governance of non-financial risks at the Bank of England (the Bank), 2023

Notes

- 1 The Court is the Bank's board of directors.
- 2 Non-financial risks are risks to the Bank's operations or reputation that would not directly affect its balance sheet.
- 3 The 'three lines of defence' model is a standard approach widely used in risk management. The first line is responsible for owning and managing risks, and is led by business areas across the Bank in consultation with specialist 'risk custodians' that oversee each key risk type. The second line is responsible for providing oversight, support and challenge across the organisation, and the third line for providing assurance.

Source: National Audit Office review of Bank of England documentation

Figure 3

The Bank of England's (the Bank's) 'three lines of defence', 2023

The Bank has three levels of responsibility for risk management

Line of defence	Responsibility	Who is involved
First line of defence	Owens and manages specific risks and implements controls.	Governors, executive directors and directors are responsible for managing risks in their business areas. Each key risk type is also overseen by a 'risk custodian' with relevant expertise.
Second line of defence	Oversees, supports and challenges the first line, defines risk management frameworks, and reports risk updates to decision-makers.	The Risk Directorate. For compliance risks, this includes the Enterprise Risk and Resilience division (non-financial risks in general), and the Compliance division (compliance with staff policies).
Third line of defence	Provides assurance that the risk management framework is fit for purpose and is being implemented as intended.	Internal Audit, which reports its findings directly to the Audit and Risk Committee.

Note

- 1 Non-financial risks are risks to the Bank's operations or reputation that would not directly affect its balance sheet.

Source: National Audit Office review of Bank of England documentation

Risk classifications and tolerances

1.18 The Bank has defined a 'risk taxonomy', which it last updated in October 2020. This categorises non-financial risks into 19 key risk types across four principal areas: operational, legal, conduct and climate change (**Figure 4**). The compliance risks we focus on in this report are primarily covered within four of the 19 key risk types: legal risk; conflicts of interest and business ethics; outsourcing, third party, and procurement risk; and staff compliance (including privacy).

Figure 4

Classification of non-financial risks at the Bank of England (the Bank), 2023

The Bank categorises 19 key non-financial risk types into four principal areas

Principal risk area	Key risk type
Operational risks	● People
	● Physical security
	● Cyber
	● Information security
	● External communications
	● Model
	● Data
	● Technology service disruption or failure
	● Outsourcing, third party and procurement
	● Process
	● Project
	● Financial reporting and tax
	● Property infrastructure (including health and safety)
	Legal risks
Conduct risks	● Conflicts of interest and business ethics
	● Financial crime
	● Fraud and insider
	● Compliance (including privacy)
Climate change risks	● Climate change

Notes

1 The four bolded key risk types are those within the focus of this report.

2 Non-financial risks are risks to the Bank's operations or reputation that would not directly affect its balance sheet. The Bank of England also defines three key types of financial risk: credit, market and liquidity risks.

Source: Bank of England documentation

1.19 Overall, the Bank aims to keep its risk exposure low, but it accepts a risk level appropriate to achieving its policy objectives. The Bank sets quantified thresholds for individual risks, and metrics to assess and monitor whether they are being managed within acceptable levels. We assess its approach in Part Two.

Promoting a risk awareness culture

1.20 A well-designed risk management framework can only be effective if it operates well in practice. This requires a good culture of risk awareness that supports staff to understand their responsibilities and how to highlight risks or raise concerns, and to have the willingness and confidence to do so.

1.21 The Bank has highlighted the importance of risk culture in key internal documents and communications. Its risk management framework documentation and guidance explain that the Court and senior leadership set the Bank's culture, but that all staff have a role in managing risk. For compliance risks, the Bank reinforces this through an annual staff code of conduct return, which sets out the principles it expects staff to follow. The Bank's Secretary's Department commissioned the Institute of Business Ethics to externally benchmark its code of conduct in 2023. It found that the Bank's code was consistent with international good practice, well-designed, and provided clear guidance on important issues.

1.22 In 2021, the Bank conducted two exercises to assess its culture of risk awareness and speaking up.

- It interviewed staff to better understand perceptions of risk and drivers of risk culture. It found that there was not a clear message on its risk culture, and that teams could do more to encourage open conversations.
- It surveyed staff about speaking up and internal whistleblowing procedures. Since 2019, Bank staff have raised fewer than 10 whistleblowing cases a year.² The Bank found that 51% of survey respondents felt that any concerns they raised would be addressed, and 39% were aware of the Bank's whistleblowing arrangements. By comparison, the 2021 Civil Service People Survey asked similar questions of staff in central government bodies; it found that 76% of respondents (the median, with most organisations ranging from 63% to 85%) were confident their concerns would be investigated properly and 68% were aware of how to raise a concern. While the results are not directly comparable due to different questions and methodologies (see Appendix One), they indicate there was less confidence among Bank staff that concerns would be addressed.

² This only includes those concerns raised by internal whistleblowers and not any concerns covered by other Bank policies and procedures, such as staff grievances. It also does not include cases of external whistleblowers relating to the financial sector, which are dealt with by a separate function.

1.23 The Bank has acted to promote and embed a risk awareness culture, including in response to its 2021 findings. The Risk Directorate expanded its provision of risk awareness training and workshops, including for senior leaders and non-executives. It also hosts discussions and forums on risk culture, and issues guidance and communications. The Secretary's Department has similarly worked with other parts of the Bank to increase awareness of the importance of, and arrangements for, speaking up and whistleblowing. It has updated its internal whistleblowing policy, increased staff communications on the topic (including in the Governor's foreword to the staff code of conduct), and provided additional coverage in training for new starters and new line managers.

1.24 The Bank has also designed risk management processes to support a more open and collaborative culture. For example, the respective responsibilities of business areas and 'risk custodians' prompt sharing of expertise and insight across the Bank. Similarly, the Bank's Compliance division aims to take a proportionate response to policy breaches to create a healthy and open culture where staff are more likely to report incidents.

1.25 There were approximately 1,400 staff as at February 2023 (around a quarter of the Bank's headcount) who had been at the Bank less than two years. This is comparable with rates of turnover in the civil service and financial sector since the COVID-19 pandemic. A large number of new starters creates both challenges and opportunities for embedding risk awareness and a healthy risk culture. The Bank has adapted its approach to training and induction to ensure risk and compliance are a prominent feature from the beginning. It seeks to maintain this through ongoing Bank-wide communications and mandatory training.

1.26 However, it will take time to fully embed this culture, and the Bank recognises that it has more to do. Since 2022, it has included new questions on internal culture in its annual staff survey. While it is too early to assess trends, the Bank expects these questions to help it monitor progress. Its 2023 survey found that 59% of staff surveyed felt they were free to speak their mind without fear of negative consequences, and 64% felt the Bank fostered an environment where everyone can be themselves.

Continuous improvement

1.27 Continuous improvement is an important principle in risk management. Organisations need an up-to-date understanding of their environment to identify, assess and manage risks effectively. This includes learning lessons from the past and from relevant examples outside the organisation.

1.28 The Bank carries out a range of benchmarking activities on different parts of its risk management framework and individual compliance risks. This includes:

- **Ongoing engagement with other organisations:** For example, the Risk Directorate regularly engages with central banks in other countries and with other regulatory bodies in the UK to compare approaches and identify lessons. The Bank's Secretary's Department takes the same approach on governance and business ethics matters by participating in the UK Regulators Corporate Governance Forum and the Central Bank Governance Group. The Legal Directorate similarly engages with other central banks and relevant UK public bodies on approaches to legal risk.
- **Specific benchmarking exercises:** For example, in 2021 the Bank participated in a review of central banks' use of the 'three lines of defence' risk governance model. In 2022, the Bank compared its overall risk management framework with UK commercial banks, and in 2023 it commissioned external benchmarking of its code of conduct (paragraph 1.21).

1.29 Teams across the Bank also provided us with examples of specific recent changes they have made to update how they manage compliance risks. This includes updating training on risk and compliance in response to feedback, such as using real-world examples to keep training engaging and understandable. In April 2023, the Bank introduced a public register of interests for its most senior officials, which it maintains to improve transparency around potential conflicts. To make it easier for staff to understand their responsibilities, the Bank's Compliance division reduced the number of internal policies from 393 in 2020 to 78 in 2023. It has also recently introduced a new 'compliance partnership' model, where the team responsible for each staff policy is required to meet regularly with a 'compliance partner' from the Compliance division. These compliance partners can answer queries and help ensure that staff policies are clear and effective.

1.30 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. It has set plans to further improve its approach, including a programme of work in 2024-25. Its plans include improving the quality and consistency of information recorded in risk registers, better linking of risk management activities to business plans and budgets, and a more consistent process for responding to incidents. The Bank's Compliance team plans to further develop how it engages with and supports other parts of the Bank to ensure staff policies are understood and followed. The Bank also recognises that it needs to continue to identify and manage legal risks effectively to keep them within acceptable levels.

Part Two

Identifying, assessing and monitoring risks

2.1 To manage risks effectively, organisations need to understand the risks they face, the impact those risks might have, and whether action is needed to respond to them. This Part examines whether the Bank of England (the Bank) has the processes and information it needs to:

- identify new or changing compliance risks;
- assess the likelihood and impact of each risk materialising; and
- monitor risks to establish whether a response is needed.

Risk and control self-assessment

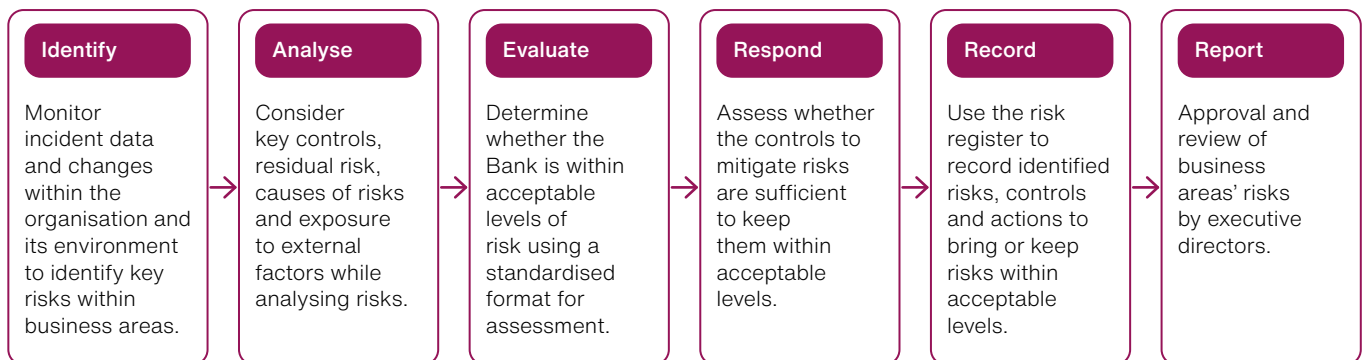
2.2 'Risk and control self-assessment' (RCSA) is a common risk management process for identifying and assessing operational risks and the adequacy of controls in place. The Bank uses a quarterly RCSA process to help create a consistent approach for business areas to identify, assess and manage key non-financial risks, including compliance risks (**Figure 5** overleaf). This sets a common standard for factors to consider, and information to provide, when identifying and assessing risks. The Bank's directors and executive directors must annually attest that they are satisfied that the risk management and control systems in their business areas are appropriate.

2.3 The Bank's RCSA process uses a consistent scoring mechanism to assess the likelihood and impact of all risks. It creates a standardised reporting format to capture information from individual business areas and at the Bank-wide aggregate level. It also provides a source of information for specialist 'risk custodians' responsible for each key risk type to analyse and identify areas that may need further action.

Figure 5

The Bank of England's (the Bank's) risk and control self-assessment process, 2023

Business areas across the Bank use the process to identify and assess non-financial risks

**Note**

1 Non-financial risks are risks to the Bank's operations or reputation that would not directly affect its balance sheet.

Source: National Audit Office review of Bank of England documentation

Identifying risks

2.4 Established principles of risk management, such as the government's Orange Book, say that risk identification should produce a holistic view of risks that may affect an organisation and its objectives.³ It should consider internal and external changes, including risks that are not under the organisation's direct control. Organisations should ensure that staff responsible for identifying risks have the necessary information, training and support.

Specialist support for risk identification

2.5 The 'risk custodian' for each key type of compliance risk is someone with relevant expertise in that area. For example, the General Counsel is the custodian for legal risks while the Chief Compliance Officer is the custodian for staff compliance risks. These custodians support business areas in several ways to identify risks.

- They provide advice, guidance, and input on risk identification in general, or on specific issues.
- They contribute to a quarterly forward-looking assessment of key risk types.
- They review risk and incident data reported by business areas to help identify trends or emerging risks. For example, any legal risks identified during the RCSA process that are new or have significantly changed are highlighted for specific discussion with the Legal Directorate.

3 HM Government, *The Orange Book: Management of Risk – Principles and Concepts*, May 2023.

2.6 The Risk Directorate aims to promote a strong risk-aware culture by supporting and challenging business areas on their risk identification. It provides guidance on how to identify emerging risks, including who to engage with and common types of emerging risk. The Risk Directorate also conducts a deep dive review on emerging risks each year for the Executive Risk Committee and Audit and Risk Committee, and runs emerging risk analysis workshops across the Bank.

Horizon scanning and external engagement

2.7 Horizon scanning refers to a range of ways in which organisations look ahead to identify potential future risks or opportunities. The Bank's Risk Directorate and risk custodians use horizon-scanning activities and engagement with other organisations to identify new or changing compliance risks and share good practice. For example:

- The Risk Directorate provides an independent forward-looking assessment of risks across all business areas, and leads a quarterly Bank-wide horizon-scanning exercise (**Figure 6** overleaf).
- The Legal Directorate engages with other organisations and stakeholders to exchange information, intelligence and ideas on legal developments. It regularly engages with legal advisers at other government organisations, central banks and regulatory lawyers around the world.
- The Privacy team is in regular contact with other regulators and central banks to discuss emerging data protection risks and their approaches to managing them.
- The Secretary's Department looks at lessons learned from other organisations, including central banks and regulators, and carries out weekly horizon scanning on where new risks may arise from.
- The Procurement team engages with other central banks and UK regulators, as well as the Bank's Legal Directorate, to identify procurement compliance risks. It used this engagement to inform a new way of operating to better manage procurement risks, which it began implementing in 2022.

Assessing risks

2.8 Once a risk is identified, it is important to assess the likelihood and impact of it materialising. Good practice in risk assessment includes having a consistent approach to assessing the level of risk, ensuring staff with appropriate specialism contribute to assessments before reporting to decision-makers, and having a clear way to test whether risks are within acceptable levels.

Figure 6

The Bank of England's (the Bank's) quarterly horizon-scanning exercise for non-financial risks

The exercise involves reviewing emerging risks within business areas and across the Bank

Stage	Description
Business area analysis	'Risk owners' within business areas across the Bank engage with staff, including expert 'risk custodians', to identify emerging risks and re-evaluate any that had been identified previously.
Review and challenge	The Risk Directorate reviews and challenges emerging risks identified by business areas to ensure none are missing, and to identify any that would be better classified as current risks.
Bank-wide analysis	The Risk Directorate analyses risks identified by business areas and compiles a list of key emerging risks across the Bank.
Reporting to risk committees	The Risk Directorate provides a quarterly risk report to the Executive Risk Committee and the Audit and Risk Committee, including analysis of emerging risks. It also provides an annual 'deep dive' report on emerging risks and how the Bank is preparing to manage them.

Note

1 Risk custodians are specialists that oversee each of the Bank's key risk types.

Source: National Audit Office review of Bank of England documentation

Risk assessments by business areas

2.9 As part of the RCSA process, business areas record and assess the compliance risks they face on the Bank's risk management information system. They do this when adding a new risk, and then quarterly. The Bank has used a new system for these purposes since January 2023, replacing 39 separate risk registers. The system links each risk to other relevant information that can help business areas make informed decisions. This includes related data on incidents and near-misses, key risk indicators and relevant controls in place to manage the risk.

2.10 We found that the information required for risk assessments by business areas is aligned with good practice. This includes the key risk type each risk relates to, who is responsible for managing it, and a description of the risk, including a quantified assessment of how likely it is to occur and what impact it might have. These quantifications produce a 'red', 'amber' or 'green' rating on a consistent basis, using the Risk Directorate's 'heatmap' (**Figure 7**). Risk assessments also include commentary and judgement on the adequacy of controls in mitigating the risk. In the compliance risk areas we examined, we found that business areas regularly update the system using a consistent approach.

Figure 7

The Bank of England’s (the Bank’s) ‘heatmap’ for non-financial risks

The Bank uses a consistent approach to assessing the impact and likelihood of each risk

Likelihood within one year

Almost certain (Above 90%)	✓		!	!	!
Likely (50%–90%)	✓		!	!	!
Possible (20%–50%)	✓	✓		!	!
Unlikely (5%–20%)	✓	✓	✓		
Highly unlikely (Below 5%)	✓	✓	✓	✓	✓
	Little or none	Minor	Moderate but short-term	Considerable but short-term	Substantial and/or sustained
	Impact				

- ! Materially beyond tolerance. Urgent and/or significant mitigating action required. Oversight by the Executive Risk Committee (ERC) and the Audit and Risk Committee (ARCo).
- Just out of tolerance. Some mitigating action required. Oversight of key issues and themes by ERC and ARCo.
- ✓ In tolerance. Managed at division or directorate level.

Note

1 Non-financial risks are risks to the Bank’s operations or reputation that would not directly affect its balance sheet.

Source: National Audit Office review of Bank of England documentation

2.11 In some cases, there were inconsistencies in the quality of information recorded, such as limited commentary to explain the assessment. In particular, we found that business areas do not always explain the cause or impact of changes where their assessment of a compliance risk is different to the previous quarter. This makes it harder for the Risk Directorate to understand the reason for the change and judge whether it needs closer monitoring or affects its Bank-wide assessment.

Bank-wide risk assessment

2.12 The Risk Directorate leads risk assessment at the overall Bank-wide level. It does this in two main ways:

- Supporting business areas' risk assessments through the RCSA process, and providing scrutiny and challenge at quarterly checkpoint meetings.
- Analysing risk data across the organisation to produce a Bank-wide risk assessment. For example, several business areas may recognise what is in effect the same risk (such as a data protection risk) for their area, or risks that may have knock-on effects on each other. To do this, the Risk Directorate uses its expertise and judgement to consolidate risks from across the Bank into a single view.

2.13 The consistent format within the Bank's risk management information system makes it easier for the Risk Directorate to review and compare risk assessments across business areas. It reports its Bank-wide risk assessment quarterly – focusing on 'amber'- and 'red'-rated risks – to both the Executive Risk Committee and Audit and Risk Committee. It also provides risk updates twice a year to the Bank's Court of directors.

Monitoring risks

2.14 Risk monitoring should help an organisation understand the extent to which the internal controls it uses to mitigate risks are working as intended. Where this is not the case, it may be because the controls are ineffective or because the nature and scale of a risk has changed. Good monitoring should provide an organisation with either confidence it is taking the right approach to keeping risks within acceptable levels, or the information it needs to take further action.

2.15 The Bank has a clear framework for monitoring and reporting compliance and other non-financial risks. Alongside its quarterly Bank-wide risk assessment, the Risk Directorate also collates a series of five to 10 'critical metrics' for each key type of compliance risk. Its quarterly risk reports present these alongside each other, providing decision-makers with different perspectives through which to monitor risks and decide whether action is needed.

Critical metrics and other risk indicators

2.16 The Bank uses 'critical metrics' to indicate the level of risk currently present and how well the controls in place are working. For example, the critical metrics for business ethics and conflicts of interest include numbers of major breaches (such as senior level conflicts that 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).

2.17 For each key risk type, the risk custodian works with the Risk Directorate to agree a set of critical metrics and provide updated figures each quarter. Where these figures represent Bank-wide metrics – for example, relating to incidents and near misses – custodians produce them using information reported by business areas across the Bank.

2.18 In the compliance risk areas we focused on, each critical metric was a quantified figure tracked quarterly or, in some cases, annually (for example, relating to the annual staff code of conduct return). For each metric, the Bank sets thresholds that define whether the metric should be rated ‘red’, ‘amber’ or ‘green’. In its quarterly risk reports, the Risk Directorate uses these ‘RAG’ ratings of individual metrics to produce an overall rating for the key risk type.

2.19 In addition to critical metrics, business areas may also monitor additional risk indicators for specific risks or groups of risks. The Bank’s new risk management information system provides information to support staff to monitor risks, and now has functionality to include metrics for each risk. The Bank told us that some business areas had progressed further than others in using risk indicators and wider metrics. This is, in part, due to the system being relatively new. The Bank told us it is supporting business areas to develop and use indicators and metrics, and plans to maintain this on an ongoing basis.

Risk appetite and tolerance

2.20 Risk appetite and risk tolerance describe the levels of risk an organisation can accept. To decide whether action is needed, organisations need to clearly define these levels, against which their assessment and monitoring can be compared. For compliance risks, the Bank has a very low tolerance for deliberate breaches and a proportionate response to other breaches based on the potential impact on the Bank’s credibility and effectiveness.

2.21 For each of its principal areas of risk, the Bank sets out the exposure level it is willing to accept to achieve its mission. The Bank has zero tolerance for deliberate breaches of statutory, regulatory or legal requirements. Otherwise, it takes a “proportionate and robust approach” to legal risks. For example, in novel or complex procurement cases, the Bank told us that the nature of procurement regulations makes it impossible to eradicate all legal risk, but that its Legal Directorate works with the Procurement team to provide robust advice for making informed decisions. Similarly, if staff conduct or compliance with internal policies fall below expected standards, the Bank aims to deal with the behaviour in a proportionate way.

2.22 The Bank primarily applies risk appetite and tolerance at two levels.

- When assessing risks through the RCSA process, the Bank uses a consistent framework for assessing whether a 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.
- For each critical metric, the risk custodian responsible works with the Risk Directorate to agree quantified thresholds to determine whether and how far the metric is within or outside acceptable levels. Setting these is a matter of judgement, and each threshold is ultimately agreed by the Audit and Risk Committee. We did not review the rationale for individual risks. In the areas of compliance risk we examined, we found that there was a consistent process to quantify thresholds for critical metrics, and that they were well aligned to the Bank's overall approach.

Part Three

Responding to risks effectively

3.1 This Part examines whether the Bank of England (the Bank) responds to compliance risks in a way that supports timely and effective decisions, and uses lessons to improve its approach. It covers:

- the controls the Bank uses to respond to compliance risks and how well it knows whether they are operating effectively;
- the Bank's actions to bring compliance risks within acceptable levels; and
- how the Bank learns from incidents and near misses, and whether it knows how well changes it makes to its approach are working.

Controls

How the Bank uses controls to respond to risks

3.2 Controls are actions, tools and processes intended to reduce the likelihood of a risk materialising or the impact it would have if it materialised. The Bank uses a range of controls to keep risks within acceptable levels. This includes, for example, processes to ensure procurement decisions are informed by legal advice where relevant, and regular reminders to staff about their responsibilities on data protection and conflicts of interest.

3.3 Business areas are responsible for identifying risk management controls, implementing them, and ensuring they operate effectively. Business areas document the controls in place to manage each risk in the Bank's risk management information system. In doing so, they set out their assessment of the adequacy of each control individually. They also assess each risk with and without all relevant controls, to indicate how effective the controls are expected to be in combination.

3.4 We found that the Bank has a good understanding of its controls to manage compliance risks. The Risk Directorate has a clear Bank-wide view of the key controls in place, which are now documented on the same information system. Specific areas we examined produced additional documentation on key controls, such as the Legal Directorate and Compliance division as custodians for legal and staff compliance risks, respectively. As part of a programme of work initiated in 2022, the Compliance team has worked with staff policy owners across the Bank to identify 465 controls used for its key internal policies and standards. The Risk Directorate has also begun work to identify key controls that cut across different risks and business areas, which it intends to complete during 2024. The Compliance team and wider Risk Directorate are working to remove duplicate controls, map each control to specific policies, and upload this information on its information system.

Understanding whether controls are complete and operating effectively

3.5 To mitigate risks effectively and efficiently, organisations should assess and test, on a regular basis, whether key controls are appropriately designed and operate effectively. Good practice is to be clear on the specific responsibilities that different parts of the organisation have regarding this testing and what level of assurance they provide. Where weaknesses are identified, organisations should act promptly to address them.

3.6 The Bank's three lines of defence (paragraph 1.16) are all responsible, to different degrees, for assessing whether its controls are designed and operating effectively (**Figure 8**).

3.7 The Bank does not yet routinely test the operating effectiveness of all its key controls to manage compliance risks. It is developing a central record of when each key control was last tested and what the outcome was, which it aims to complete by the end of 2023-24. The Bank told us that some areas, such as the Legal Directorate, already test and document the operating effectiveness of controls, but this is not yet routine and outside the Legal Directorate there are some key controls for which there is no evidence of such testing. The Bank's plans for 2024-25 include implementing a risk-based approach to prioritise controls for testing. The Compliance division also plans to use the better information it now has on controls to test their effectiveness, focusing on higher-risk areas.

Figure 8

Responsibilities for assessing risk management controls at the Bank of England (the Bank), 2023

The Bank's 'three lines of defence' are all responsible, to different degrees, for assessing whether controls are appropriately designed and operating effectively

Lines of defence	Responsibilities
First line (business areas)	<p><i>Assessing that the controls they implement are operating as intended.</i></p> <p>The Bank told us that some parts of the Bank – such as the Legal Directorate – conduct formal programmes of work to test key controls, but not all key controls are yet routinely tested.</p>
Second line (Risk Directorate)	<p><i>Supporting, overseeing and challenging business areas on the effectiveness of controls and mitigating actions.</i></p> <p>This includes, for example, testing the effectiveness of controls to ensure staff comply with key internal policies.</p>
Third line (Internal Audit)	<p><i>Evaluating controls to provide assurance that they are appropriate and effective.</i></p> <p>Internal Audit chooses which areas to focus on, based on: its assessment of risks across the organisation and the strength of the controls to mitigate them; other work carried out within the Bank, by its Independent Evaluation Office, or by external auditors or reviewers; and input from internal management and external stakeholders.</p>

Source: National Audit Office review of Bank of England documentation

3.8 The Bank's Internal Audit function provides assurance on key areas of risk, including how well controls are working. This function focuses on areas based on its assessment of risks across the organisation and how strong it expects the relevant controls to be. We found that the Bank acts in response to Internal Audit's recommendations. In our areas of focus, Internal Audit has, since 2020, issued satisfactory ratings to some areas of risk management and the work of the Legal Directorate. It has also issued four reports in the same period that identified improvement needs, which covered procurement, data privacy, and operational risk management and compliance in specific business areas. We saw evidence of the Bank taking action in response to Internal Audit's recommendations, most of which it had implemented by the end of 2023.

3.9 The Bank has not carried out an assurance-mapping exercise on compliance risks. Assurance maps are visual illustrations that provide an overview of the completeness of an organisation's controls and help highlight any gaps or duplication. They typically show: the areas on which an organisation requires assurance (such as business processes, risks, controls or risk management activities); the teams or control activities, across the three lines of defence, that provide assurance over each area; and the level of assurance provided by each team or activity. Government's guidance on risk management recommends that public sector organisations carry out assurance mapping.⁴

Bringing risks within acceptable levels

3.10 Organisations should have clear plans to bring risks within acceptable levels. While achieving this may take time, organisations can track changes in relevant risk indicators to gauge whether their plans are likely to be successful, or whether they need to take additional action.

3.11 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, resulting in a 'red' rating. The Bank defines minor breaches as "unintentional acts or omissions which, individually, have minimal impact". Its risk management framework describes how risk custodians should develop and oversee specific action plans to bring 'red'-rated critical metrics back within acceptable levels.

3.12 For example, in its September 2023 risk report to the Audit and Risk Committee, the Bank set out an action plan to address levels of breaches with staff policies. Its critical metric for minor breaches (of any staff policy) had been rated 'red' – more than 100 breaches – in each of the previous four quarters. The Bank told us that the vast majority of breaches are self-reported by Bank staff. In the latest quarter, nearly half the breaches involved emails being sent to the wrong addresses. Most of the rest related to conflicts of interest policies, including late disclosures or retrospective approvals for personal financial transactions such as mortgages or investments.⁵ Major compliance breaches had also increased to 12 in the quarter to August 2023 and were rated 'red'. The Bank deals with individual major breaches firmly, typically involving a warning or disciplinary action, while it aims to deal with accidental minor breaches in a way proportionate to the impact. In total, there were 628 minor and 28 major compliance breaches over the year to August 2023, compared to 584 minor and 19 major breaches in the previous year.

⁴ HM Government, *The Orange Book: Management of Risk – Principles and Concepts*, May 2023.

⁵ For personal financial transactions, the Bank's code of conduct states: "Our own savings, investments and borrowings sometimes give us a personal interest in decisions that are to be made by the Bank; and it is important to show that our own decisions about investments are not influenced by information that we know only as a result of working here, which is often not in the public domain."

3.13 The Bank's action plan set out what it was doing to bring down numbers of compliance breaches. This includes educating staff on the Bank's policies and updating some policies, including on working from abroad, to make them clearer. The Compliance division is responsible for implementing the plan in coordination with other parts of the Bank. This includes business areas and owners of relevant staff policies, such as the Bank Secretary as risk custodian for conflicts of interest. However, this plan is new, and their impact is not yet known. The Compliance division is also working to implement a stricter approach to deal with persistent delays in completing mandatory tasks, such as expense reconciliations and mandatory training.

Learning

Learning from incidents and near misses

3.14 The Bank defines an incident as an event which has an actual or potential impact on the smooth functioning of the Bank in delivering its mission. For example, incidents may include emailing confidential information to the wrong recipient, accepting gifts without prior approval, or purchasing services in breach of procurement law or internal policies. The Bank defines a near miss as an event that is averted, but not through the operation of normal controls. Good practice in risk management is to record incidents and near misses promptly, review responses to identify successes and failures, record lessons in a form that employees find open and accessible, and embed lessons by improving controls or other activities.

3.15 Bank employees are required to report incidents and near misses in a timely way and identify the actions that will resolve them and prevent re-occurrence. Teams across the Bank can input an incident or near miss to its risk management information system. They are required to do so within two working days of identifying the incident. The system includes dashboards for the Risk Directorate to track incidents and identify areas where most or increasing numbers occur. The Risk Directorate may also commission post-incident reviews, depending on the actual or potential impact. The Bank aims to respond to compliance breaches in a proportionate way, which avoids a culture of fear where staff are reluctant to report incidents or near misses.

3.16 The Bank has separate processes for learning from 'critical incidents'. The Bank defines these as incidents that require direct involvement from senior leaders. The Bank conducts post-incident reviews of all critical incidents and reports major incidents to the Executive Risk Committee on a quarterly basis. The Bank has an Incident Review Forum that supports the Executive Risk Committee by examining:

- how the Bank has managed incidents of note, including whether lessons have been shared appropriately;
- broader trends in incidents at the Bank and their implications; and
- the potential impact of incidents in other organisations.

3.17 We saw examples of the Bank taking action to implement learning points from both major and minor incidents. Following high-profile incidents in 2017 and 2019 (paragraph 1.3), the Bank conducted formal reviews and overhauled its approach to managing non-financial risks. We also saw evidence of the Bank's processes for minor incidents operating as intended. This included the Risk Directorate reviewing data protection incidents and reporting them to the Audit and Risk Committee, the Incident Review Forum discussing them, and the Bank implementing actions to prevent re-occurrence.

Learning from the Bank's own interventions

3.18 Evaluation is a systematic assessment of the design, implementation and outcomes of an intervention, to provide insights into how it has been implemented and what effects it had. These insights support accountability for decisions and can help decide whether interventions should be continued, expanded, improved or reverted.⁶

3.19 The Bank has made changes to improve how it manages compliance risks but does not routinely evaluate how well the changes are working. The Bank uses its risk monitoring to consider the overall effectiveness of its approach, and whether further improvements are needed. It has also conducted some recent evaluations, including benchmarking its approach against other organisations. In 2021, for example, it evaluated the impact of its new risk management arrangements as part of responding to an external survey by the Bank for International Settlements. However, the Bank does not set an expectation that changes to risk and compliance arrangements be formally evaluated. More systematic review could help the Bank maximise how cost-effective its risk management interventions are.

3.20 The Bank's Independent Evaluation Office was established in 2014 to operate at arm's length from other areas of the Bank and assess the Bank's performance. It has published 10 evaluations to date. Compliance risks have not been a focus of its work so far but, in 2017, it supported the non-executive directors' review of the Bank's approach to conflicts of interest.

⁶ HM Treasury, *Magenta Book: Central Government guidance on evaluation*, March 2020; Comptroller and Auditor General, *Evaluating government spending*, Session 2021-22, HC 860, National Audit Office, November 2021.

Appendix One

Our audit approach

1 This study examined whether the Bank of England (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’ throughout the report). Within these areas, we focused on compliance risks relating to how the Bank functions as an organisation that could affect its credibility and effectiveness if not managed well. The Bank relies on public trust and its reputation for integrity to carry out its role to promote the good of the people of the UK by maintaining monetary and financial stability.

2 Our study covered:

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

3 Our assessment was based on common principles of effective risk management, for example, as set out in the government’s Orange Book.⁷ It was also informed, where relevant, by findings from our past work and by risk management practice we have seen in other organisations. Our independent conclusions were reached following an analysis of evidence collected primarily from September to December 2023.

4 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. 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.

⁷ HM Government, *The Orange Book: Management of Risk – Principles and Concepts*, May 2023.

Our evidence base

Case studies

5 Rather than 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. This allowed us to examine how the Bank's approach to risk management is applied in practice.

6 We selected our case studies to examine areas that are important to the Bank's credibility, and which provided us with coverage of legal, ethical and staff policy compliance risks. The case study areas involved the full range of methods set out in the rest of this Appendix, including specific interviews and walkthroughs with staff, and a review of relevant documents and data.

7 Our case study areas were:

- conflicts of interest;
- data protection and privacy;
- procurement, including compliance with procurement law and inappropriate use of resources; and
- internal whistleblowing.

Interviews with Bank of England staff

8 We conducted semi-structured interviews with staff at the Bank responsible for risk management in general, and for managing the areas of legal, ethical and staff compliance risk we focused on. This included the Chief Operating Officer's office, various teams within the Risk Directorate (including the Compliance division, Enterprise Risk and Resilience division, and Privacy team), the Secretary's Department, the Legal Directorate, and the Procurement team.

9 We used interviews to obtain an understanding of: how the Bank approaches risk management in general and in relation to compliance risks; how its documented processes work in practice; and what its plans are to continue developing how it manages compliance risks. Some interviews involved an element of walkthrough, for example, where interviewees described processes or showed us the Bank's risk management information system. We triangulated interviews with other evidence sources where possible, including document review.

Document review

10 We reviewed a range of published and unpublished documents that the Bank provided to us. These primarily included the following.

- **Documents relating to the Bank’s overall risk management approach:** This included the Bank’s risk management framework, risk taxonomy, and the terms of reference for its key risk management governance committees. It also included minutes and papers from the Bank’s Audit and Risk Committee.
- **Documents demonstrating how the Bank seeks to ensure understanding and a culture of risk awareness among staff:** This included guidance and policies, training and workshop materials, and the Bank’s code of conduct. It also included staff survey results, including relevant extracts from the Bank’s overall staff survey as well as findings from its 2021 survey on speaking up and internal whistleblowing arrangements.
- **Documents relating to how the Bank identifies and manages compliance risks in practice:** For our areas of focus, this included relevant risk registers, quarterly monitoring reports with ‘critical metrics’ for each key risk type, logs of incidents and near misses, and Internal Audit reports. It also included key risk papers provided to the Bank’s Audit and Risk Committee and Court of directors.
- **Documents relating to how the Bank seeks to continuously improve its approach to managing compliance risks:** This included outputs from several benchmarking exercises the Bank has conducted or participated in, and work currently underway or planned for 2024-25.

11 We also reviewed additional documentation on the Bank’s wider work, including its annual report and accounts, and its website, to understand the wider context within which it seeks to manage compliance risks.

Literature review

12 We conducted a web-based literature review to gather information on compliance and other non-financial risks relevant to the Bank and similar organisations. We used this review primarily to scope and design the study, including determining what information to request of the Bank and shortlisting a sample of case studies. This included our past reports on a range of public bodies, reports from parliamentary select committees and other commentators, and news articles.

13 We also used a literature review to help us establish evaluative criteria (what ‘good’ looks like) with which to assess the Bank’s systems and processes. This was drawn from a range of sources, such as other organisations’ frameworks, code of conduct and relevant policies, the UK Corporate Governance Code, and established guidance on risk management (including the ‘ISO 31000’ standards and government’s Orange Book). We also used past National Audit Office (NAO) reports and guidance to inform our evaluative criteria.

14 To benchmark the findings from the Bank’s 2021 staff survey on speaking up and internal whistleblowing, we compared these with findings from the 2021 Civil Service People Survey, which asked similar questions. We note in the report (paragraph 1.22) that the results are not directly comparable due to different questions and methodologies.

- The Bank of England staff survey on speaking up received responses from 1,873 people, a 40% response rate. The exact statements staff were asked to agree or disagree with were as follows:
 - “I am aware of the Bank’s Speak Up (whistleblowing) policy and procedures.”
 - “I am confident that if I raised a concern under the Bank’s Speak Up (whistleblowing) policy and procedures, it would be addressed.”
- The Civil Service People Survey involved 102 central government bodies. A total of 536,096 people were invited to take part and 346,957 participated, a 65% response rate. The results we describe in paragraph 1.22 are the medians, while the range provided is from the 5th to the 95th percentile by organisation. The exact questions were as follows:
 - “Are you aware of how to raise a concern under the Civil Service Code?”
 - “Are you confident that if you raise a concern under the Civil Service Code in [your organisation] it would be investigated properly?”

15 In paragraph 1.26, we also describe results from the Bank’s 2023 overall staff survey. We did not benchmark this against central government as there were not sufficiently comparable questions in the Civil Service People Survey. The Bank’s 2023 staff survey received responses from around 3,800 people, a 73% response rate. The exact statements staff were asked to agree or disagree with were as follows:

- “SPEAK MY MIND: I feel free to speak my mind without fear of negative consequences.”
- “PSYCHOLOGICAL SAFETY: The Bank fosters an environment where everyone can be themselves.”

Engagement with internal experts

16 We engaged with experts within the NAO to help design the study and our evaluative criteria, and to quality-assure our findings and ensure our assessment was fair. This was primarily with experts in financial and risk management, who supported the study throughout. We also sought input on specific aspects of our study from our policy and legal team, our risk and internal audit teams, and experts in procurement and in people and operational management.

This report has been printed on Pro Digital Silk and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.



National Audit Office

Design and Production by NAO Communications Team
DP Ref: 012683-001

£10.00

ISBN: 978-1-78604-539-3