National Audit Office

REPORT

Risk management in government: improving capability and decision-making

Cross-government

SESSION 2026-27
18 NOVEMBER 2026
HC 768

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 2025, we recognised £2.6 billion of positive financial impacts from our past work through reduced costs, improved service delivery, or other benefits to citizens. This represents about £24 for every pound of net expenditure.

National Audit Office

Risk management in government: improving capability and decision-making

Cross-government

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 16 November 2026

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

9 November 2026

HC 768 | £10.00

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.

018285 11/26 NAO

© National Audit Office 2026

Contents

Key information 4

Summary 6

Part One
Risk management capability and systems 16

Part Two
Culture, leadership and influence 25

Part Three
Using risk management to inform decision-making in practice 35

Appendix One
Our audit approach 43

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:

John Anderson, Ross Coron, Lana Eekelschot and Alberto Vanzo, with specialist input from Mfon Akpan and Emily Stanyon and the assistance of Matthew Doole, Richard Kelso, Kevin Mateescu, Tilly Meers and Oliver Steward, under the direction of Rich Sullivan-Jones.

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 information

Why risk management matters



- The government operates in an uncertain, complex and interconnected environment.
- Delivering public services and securing value for money increasingly depend on how well the government understands, manages and responds to risk and uncertainty.
- Public bodies are expected to take well-managed risks to support innovation and improve public services.

Who is responsible



- Those responsible for delivering objectives and services manage risk day to day, specialist functions provide oversight and challenge, and internal audit provides independent assurance.
- The accounting officer provides leadership for risk management, supported by the Board and the Audit and Risk Assurance Committee.
- The *Orange Book* sets cross-government principles, while the Risk Centre of Excellence, based in HM Treasury, works to improve risk management across government.

What we did



We assessed how well government bodies manage risks through interviews, case studies, a survey of risk professionals, focus groups with them, a review of our previous work and expert insights.

What we found



The government has strengthened the foundations of its risk management through improved guidance and systems, but further progress is needed to translate these improvements into better decisions and outcomes.

Government bodies have improved the foundations of risk management, but progress remains uneven and some practices are not yet consistently used.

- The government has strengthened its guidance and training on how to manage risks, but there are gaps in how organisations evaluate options, use information and check whether risks are managed effectively.
- Risk teams within government bodies generally consider that they have the skills they need.
- Many organisations have moved from spreadsheets to dedicated risk management systems but are at different stages in realising their benefits.

What we found *continued*



Risk management is not consistently integrated into leadership, governance and decision-making across government.

- Senior leaders' engagement with risk management as a key element in effective decision-making remains inconsistent.
- Risk professionals are often involved too late, or do not have enough influence, to help shape major decisions.
- Risks are not always mitigated or escalated early enough, with a 'good news' culture persisting in some areas.

Government bodies are not yet responding consistently to emerging, persistent and cross-cutting risks.

- Government bodies often identify emerging and evolving risks, but do not consistently translate this insight into timely action.
- Government bodies are increasingly setting out their risk appetite (the amount of risk they are willing to seek or accept), but this does not always lead to effective action.
- Government bodies often lack the oversight, coordination and levers needed to effectively manage risks affecting more than one organisation.

What the government needs to improve



Our report makes recommendations for the centre of government and highlights approaches government bodies can take to make further progress in managing risks effectively, including:

- strengthening leadership and capability;
- embedding risk in decision-making; and
- managing risks across organisational boundaries.

Summary

1 Effective risk management helps the government achieve its objectives and secure value for money. In an increasingly uncertain and interconnected environment, it supports better decision-making, innovation, adaptability and public service resilience. Conversely, weaknesses in risk management can lead to poorer public service delivery, delays and avoidable costs. **Figure 1** provides examples of how risk management can affect costs and outcomes. Our good practice guide *Overcoming challenges to managing risks in government* sets out key components of effective risk management and why they matter.[1]

Figure 1

Examples of how risk management can affect costs and outcomes

Effective risk management supports innovation and public service resilience, whereas weaknesses can lead to substantial cost or disruption

Example	Event	Consequence
Securing COVID-19 vaccines 	During the COVID-19 pandemic, the government identified the risk that conventional approaches to securing vaccines would delay access, and the opportunity to accelerate delivery. Through the Vaccine Taskforce, the government managed uncertainty by investing in a diverse portfolio of vaccine candidates.	The government secured supply of several potential vaccines before clinical outcomes were known. This allowed it to deploy vaccines quickly once they were approved.
British Library cyberattack 	In October 2023, the British Library experienced a cyberattack. The Library had identified risks from increasing third-party access to IT systems and planned stronger security controls, but the attack occurred before they were implemented.	The attack disrupted the Library's research and digital services and affected its data and systems. The incident required substantial resources to restore services and strengthen cyber resilience over an extended period.

Source: National Audit Office analysis of its back catalogue and publicly available documents

1 National Audit Office, *Overcoming challenges to managing risks in government*, December 2023.

2 Risk management is particularly challenging in government because many of the most significant risks it faces are complex and interconnected. They require coordinated action, difficult trade-offs and effective decision-making under conditions of uncertainty. Risks can cascade and compound, increasing their impact and making them harder to manage. The range of risks the government faces includes:

- emergencies such as pandemics, extreme weather events and national security incidents;
- operational risks such as workforce pressures, cyber incidents and fraud;
- policy and delivery risks such as failing to complete projects or achieve intended outcomes; and
- long-term threats such as climate change.

3 The government's risk environment has become more complex and uncertain. Recent events, including the COVID-19 pandemic, geopolitical instability, economic disruption and climate impacts such as wildfires, have highlighted weaknesses in the government's ability to anticipate and respond to system-wide risks. At the same time, the government increasingly expects public bodies to take well-managed risks to support innovation and improve public services.

4 Risk management is a shared responsibility across all levels of government bodies, involving operational staff, risk professionals, senior leaders and assurance bodies. Paragraph 1.2 sets out their roles and responsibilities.

5 The government has made changes in recent years to strengthen and professionalise risk management. It has updated guidance, including substantial revisions to the *Orange Book* on risk management, strengthened the treatment of risk in wider government guidance and standards, established the Government Risk Profession and expanded risk training. The government's Risk Centre of Excellence (CoE) supports this profession through guidance, training and networks for risk professionals.

Scope of this report

6 This report assesses how well central government bodies manage risks to make better decisions and improve public service delivery. While it does not assess the overall value for money of government spending on risk management, it makes recommendations to improve practices across government. It covers:

- risk management capability and systems (Part One);
- risk management culture and leadership, and risk professionals' influence (Part Two); and
- how government bodies use risk management to inform decision-making in practice (Part Three).

7 This report focuses on central government departments and arm's-length bodies (ALBs). It does not assess risk management in the devolved administrations, local government, government-owned companies, or cross-government risk management arrangements such as the National Security Risk Assessment, which we have covered in previous work. While we considered the Risk CoE's role in setting expectations and supporting risk management, we did not evaluate its performance.

8 In this report, we define risk as the effect of uncertainty on the government's objectives. These effects may be negative (threats) or positive (opportunities).

Key findings

Risk management capability and systems

9 Government bodies are improving their risk management arrangements through better policies and information systems. The government has strengthened its central guidance in recent years and has a well-developed set of principles, requirements and guidance to help departments and ALBs manage risks. Risk professionals across government find these resources valuable, and would welcome more support to identify, assess and manage opportunities. Many organisations have transitioned from tracking risks manually to risk management information systems. These can improve oversight by highlighting overdue actions and giving senior leaders clearer information to scrutinise how risks are managed. Organisations are at different stages in realising their benefits (paragraphs 1.5, 1.6, 1.8 and 1.10, and Figure 4).

10 Progress in adopting good risk management practice remains uneven across government, with common gaps in the use of information and assuring that risks are being managed effectively. For example, government bodies do not typically consider the chances of different degrees of success and failure when assessing options. Government bodies are not yet making full use of performance information and early warning indicators to anticipate and monitor risks, limiting the quality of risk reporting and the speed of response. Many government bodies do not know, with confidence, whether risks are being managed effectively and efficiently across the organisation, as techniques such as assurance mapping are not always in place or fully developed (paragraphs 1.9 to 1.12).

11 Risk teams generally consider that they have the skills they need. Risk teams are often small relative to the size and complexity of the organisations they support. Of the 62 risk professionals in central government who responded to our survey question on skills, 84% said their team has adequate skills and expertise to support effective decision-making. Risk professionals told us that improving risk capability across their organisation is a higher priority than increasing resources or expertise within central risk teams. Risk teams have used tailored training, business partnering and 'risk champion' networks to strengthen risk awareness across their organisations. However, organisations do not consistently identify and plan for future risk resourcing needs, which may reduce their effectiveness over time (paragraphs 1.13 to 1.16).

Culture, leadership and influence

12 Senior leaders' engagement with risk management as a key element in effective decision-making is inconsistent, which can mean organisations are more exposed to risks, or miss opportunities to improve services. While we observed examples of good risk leadership, risk and governance professionals told us some leaders do not view risk management as enabling informed decision-making and give it limited priority in governance forums. Reasons include insufficient understanding of the value of risk management and of leaders' responsibilities for managing risks, a perception that risk management hinders delivery, and overly technical risk reporting that is not focused on decision-makers' needs. Audit and Risk Assurance Committees provide important oversight and challenge, but skills gaps among committee members in evolving areas such as cyber security, digital transformation, artificial intelligence and climate change can constrain their effectiveness (paragraphs 2.7 to 2.9, 2.17 and 2.18, and Figure 6).

13 Risk professionals' ability to add value to major decisions is often constrained by late involvement. Risk professionals often lack influence as they are brought in too late to shape options. In our survey, 58% of respondents said risk professionals are typically brought in either too late to shape decisions, mainly to provide assurance and sign-off, or not at all. We found limited evidence of major decisions or organisational direction changing because of input from risk professionals. In hierarchical organisations, the often low seniority of those leading risk teams can also restrict their access to senior decision-making forums. The number of Chief Risk Officers in central government departments more than doubled, to 11, between 2016 and June 2026. Risk professionals offered mixed views on whether this role helps increase the influence of risk teams (paragraphs 2.11 to 2.13 and Figure 7).

14 There has been improvement across government in encouraging a culture of raising concerns, though this remains uneven. We reported in 2025 that the Bank of England's Real-Time Gross Settlement digital transformation programme fostered a transparent 'no surprises' culture that encouraged staff to raise concerns, which was an important enabler of delivery. In our survey of risk professionals, 71% of respondents said their organisation had a healthy culture that enables risks to be discussed openly and honestly. The Civil Service People Survey shows that civil servants' confidence in speaking up when they identify a serious policy or delivery risk increased from a median score of 66% in 2017 to 75% in 2021 and has remained broadly stable since. Variation between organisations has reduced since 2017 but substantial differences remain (paragraph 2.5 and Figure 5).

15 Key risks are not always mitigated or escalated promptly, with a 'good news' culture persisting in some areas. The government expects that staff at all grades, as well as ministers, play a role in managing risks, and the Risk CoE has developed training and learning resources to improve risk awareness among non-risk professionals. However, in our survey, only 58% of respondents said people in their organisations view identifying risk as everyone's role. Risk professionals told us the effectiveness of those in charge of risks is variable. Several government bodies have significant backlogs of outstanding mitigating actions, indicating that risks are not always addressed promptly. We heard that risk management is sometimes treated as a compliance exercise and that delivery pressures can cause risk management activity to be deprioritised. A 'good news' culture can also discourage open discussion and escalation (paragraphs 2.15 and 2.16).

Using risk management to inform decision-making in practice

16 While government bodies identify emerging and evolving risks, they are often slow to respond. Many organisations use horizon scanning and scenario planning to anticipate issues, and some focus on the long-term trends that might affect their ability to deliver services. For example, the Ministry of Justice has assessed the civil emergency risks most likely to materialise over the next six months and analysed global long-term trends that may affect it over the next five to fifteen years. However, timely action across government in response to emerging and evolving risks is inconsistent and often lacking (paragraphs 3.3 and 3.4).

17 Government bodies are increasingly articulating their risk appetite (the amount of risk they are willing to seek or accept), but they are not yet consistently using it to inform decisions on funding and resourcing. A clear risk appetite gives staff confidence to test new approaches and improve services, whereas uncertainty about what risks are acceptable can inhibit innovation. For example, the Department for Work & Pensions told us a higher risk appetite for innovation during the COVID-19 pandemic helped accelerate the development of new approaches to improving compliance of child maintenance payments. These approaches helped prevent an estimated 715 cases a month from falling into arrears. However, risk appetite is still often not used to shape investment and resourcing decisions, with only 47% of respondents to our survey saying their organisation uses risk appetite to inform decisions. In June 2026, most central government departments reported that the majority of their principal risks were outside their stated risk appetite or tolerance, often for multiple years. This may indicate that their risk appetite does not accurately reflect the level of risk they are prepared to accept, or that actions to bring risks within appetite are ineffective or constrained. For example, legacy technology and specialist staff shortages may constrain departments' ability to bring cyber security risks within appetite. Officials told us funding constraints and concerns about accepting greater exposure to serious harm can make it difficult to align persistent risks with their stated appetite (paragraphs 3.5 and 3.7).

18 Government bodies often lack the oversight, coordination and levers needed to manage risks that cut across organisational boundaries. They often have a limited understanding of how risks interact and how issues in one area can affect others. Departments' oversight of ALB risks is inconsistent. This limits their ability to challenge ALBs, support them before issues escalate, and understand how risks across organisations may compound and affect outcomes for which the department is accountable. For example, some ALBs told us they had limited contact with their sponsoring department's risk team, reducing both sides' ability to develop a shared view of risks. Limited oversight of project, programme, delivery partner and supplier risks also hinders government bodies' ability to anticipate and respond to disruptions. Many significant risks facing departments require cross-government collaboration, but those responsible for managing them often lack the authority, levers or incentives to do this in an integrated way. Addressing these challenges will become increasingly important as central government transfers more responsibilities to mayors and local government (paragraphs 3.8 to 3.12).

19 Government bodies are taking steps to learn, improve and innovate in how they manage risks, but could do more to make these efforts more systematic and increase their impact. We found examples of organisations reviewing incidents and near misses to learn from experience and improve practice. The Risk CoE provides tools and guidance to help organisations improve how they manage risks, and risk teams are beginning to use artificial intelligence to improve efficiency and support decision-making. However, opportunities remain to make improvement efforts more systematic and targeted. Government bodies do not routinely have robust, documented risk management improvement plans, making it harder to target improvement, monitor progress and embed learning. There is also no government-wide assessment of risk management effectiveness to provide a consistent basis for identifying leading practice and areas for improvement across government (paragraphs 3.13 to 3.18).

Conclusion on value for money

20 Managing risks effectively is critical to achieving the government's objectives and securing value for money in an uncertain and highly interdependent environment. It helps the government become more resilient to increasingly complex threats and it supports well-managed risk-taking to innovate and improve services. Many government bodies have strengthened their risk management arrangements in recent years, supported by the work of the Risk CoE.

21 However, most progress has been in improving the tools, frameworks and processes used to manage risks. While these are important foundations, they are not sufficient on their own. Effective risk management requires supportive leadership and an organisational culture that encourages informed risk-taking and open discussion of concerns, and it needs to be embedded in how government bodies set priorities, make decisions and allocate resources. Although we have found examples of good practice across government, progress is uneven, with significant variation in the extent to which organisations use risk management to inform decisions, manage risks that cut across organisational boundaries, and respond effectively to emerging threats and opportunities.

What government bodies can do to overcome challenges to managing risks

22 Ensuring that the government manages risks effectively and consistently to secure value for money and improve public services will require sustained effort across organisations, underpinned by effective support from the centre of government. Our good practice guide *Overcoming challenges to managing risks in government* sets out 10 approaches that government bodies can take. Our work for this report has reinforced their continued relevance to the persistent challenges government bodies face. **Figure 2** on pages 14 and 15 presents these approaches and complements our new recommendations for the centre of government. The government has issued a wide range of guidance, tools, training and learning resources to help organisations put these approaches into practice.

Recommendations for the centre of government

23 To improve the government's ability to manage risks effectively in practice, HM Treasury should ensure that the Risk CoE has the levers and capacity to:

a work with the Project Delivery Function to improve how government bodies assess risks in option design and appraisal, including by more consistently estimating the likelihood of different degrees of success and failure;

b increase its engagement with other government functions and professions to help ensure that commercial, digital, financial, grant management, operational, policy and workforce decisions are informed by risk; and

c regularly review and challenge departments' and large ALBs' plans for improving risk management, including future resourcing and skills, and support their development and implementation.

24 To strengthen leadership for risk management across government, the Risk CoE should engage with the Cabinet Office, given its role in civil service leadership, capability and talent development, to:

d ensure that senior civil service capability and performance frameworks reflect the leadership behaviours needed to support effective risk management;

e set clear, role-specific expectations for risk training for new non-executive directors, senior civil servants, permanent secretaries, and equivalent roles in ALBs, building on the Risk CoE's existing training offer;

f set clear expectations for how cross-government learning and development initiatives will prepare current and future leaders to manage risks effectively; and

g design and deliver the training and development activities needed to meet these expectations.

25 As the government develops arrangements to support further devolution, the Ministry of Housing, Communities & Local Government and HM Treasury should work with the Cabinet Office to:

h set out a clear approach to identifying, escalating and responding to risks that cut across organisational, geographical and policy boundaries, including giving the centre of government visibility of risks whose combined effects could be significant.

Figure 2

Approaches to overcoming challenges to managing risks in government

Our 2023 good practice guide identified 10 approaches that the government can take to overcome risk management challenges

Approach	Why is this a priority?	What actions can organisations take?
 **1. Establish strong leadership and risk culture**	A tone from the top that establishes the importance of risk management and promotes a positive risk culture will have greater success in driving the right behaviours and actions throughout the organisation	• Set the right tone at and from the top of the organisation • Strengthen leadership, accountability, and assurance arrangements for risk management • Reduce the risk of optimism bias through independent challenge • Promote a culture of psychological safety to have open dialogue around risk
 **2. Build capability and expertise**	Developing risk management expertise and credibility will strengthen the organisation's ability to make risk-informed decisions which achieve strategic objectives and deliver value-for-money outcomes	• Assess the skills and capabilities needed and address gaps • Deliver interventions to raise risk awareness and capability across the organisation • Upskill and develop risk practitioners to strengthen risk management credibility • Engage risk experts and specialists where appropriate
 **3. Define and embed risk appetite and tolerance**	Expressions of risk appetite and risk tolerance which are understood across the entire organisation will set parameters for individuals to operate and enable risk-taking which supports the achievement of strategic objectives	• Clearly articulate the levels of risk the organisation is willing to accept and tolerate • Base risk appetite and tolerance on good information • Communicate risk appetite across the organisation so it can be understood and put into action • Flex risk appetite to reflect changing dynamics in the environment and management's preferences
 **4. Take a forward-looking view**	Anticipating future risks will enable organisations to be better prepared and more responsive to changes and shocks	• Continually scan the horizon for emerging and future risks and opportunities • Build in diversity to risk identification by including expert viewpoints • Use foresight tools and futures thinking to understand uncertainty and inform risk identification • Be imaginative in planning for severe but plausible scenarios
 **5. Make risk-informed decisions**	Decisions which are informed by robust risk management will take threats and opportunities into account so the organisation can better achieve its objectives	• Align risks with the organisation's strategy, goals and objectives • Design risk management into the governance architecture • Be deliberate about risks and opportunities in decision-making • Engage risk expertise early in the decision-making process

Figure 2 *continued*
Approaches to overcoming challenges to managing risks in government

Approach	Why is this a priority?	What actions can organisations take?
 **6. Adopt a whole-system approach**	A holistic approach to risk management enables interdependent and interconnected risks to be identified and managed in a robust and integrated manner	• Identify risks in the organisation and third-party ecosystem • Map interdependencies and connections for cross-cutting risks • Assess the range of impacts and consequences of risks • Take a joined-up approach to managing risks and break down silos
 **7. Assess risk impact**	Thorough assessment and evaluation will enable the impact of risks to be consistently understood and help prioritise the different risks the organisation is managing	• Use the right tools and expertise to assess and evaluate risks • Leverage good-quality data to support the risk assessment effort • Deploy qualitative and quantitative methods to assess impact • Identify and assess the aggregate impact of risks across the organisation
 **8. Take action to address risks**	An organisation where individuals understand their responsibilities for managing risks – and how risk appetite and tolerance can be applied in practice – will be better equipped to take effective action as risks develop	• Have clear ownership and accountability for risks • Develop appropriate responses in line with the organisation's risk appetite and tolerance • Have clear criteria for escalating risks that fall outside appetite or tolerance • Gain assurance over the effectiveness of risk management processes
 **9. Monitor and report on the risks that matter**	Continuous risk monitoring and effective risk reporting will help focus attention on the risks that should matter most to the organisation	• Set meaningful performance metrics and indicators to monitor risks • Apply tools which enable real-time and dynamic monitoring of risks • Promote timely and accurate reporting of significant risks to key decision-makers • Ensure risk registers are robust and "living documents" that reflect significant risks
 **10. Drive continuous improvement**	Learning lessons from others and assessing risk maturity will allow the organisation to continually develop and improve its approach to risk management	• Assess the current level of maturity to identify gaps and areas for development • Identify and share good practice across the organisation • Learn and share lessons from beyond the organisation • Validate, benchmark and seek assurance over risk management arrangements

Source: National Audit Office, *Overcoming challenges to managing risks in government*, December 2023

Part One

Risk management capability and systems

1.1 This part sets out:

- roles and responsibilities for managing risks within government bodies;
- the government's risk guidance, frameworks and tools, including progress in adopting good practice across government; and
- skills and expertise within government bodies' central risk teams.

Roles and responsibilities

1.2 Each organisation is responsible for managing the risks that affect it. Many government bodies adopt the 'three lines' approach, which allocates responsibility for managing risks, overseeing and challenging risk management, and providing assurance that risks are managed effectively to different parts of the organisation (**Figure 3** on pages 17 and 18).

- Primary responsibility for managing risks rests with those accountable for delivering objectives and managing activities across the organisation (the first line).
- Many organisations have a central risk team that provides expertise, guidance, oversight and challenge (the second line), and provides assurance that risks are managed effectively, although it does not generally own operational or business risks.
- Internal audit (the third line) provides independent assurance on the effectiveness of governance, risk management and the controls, checks and safeguards used to prevent or reduce risks.

Ministers set the strategic direction for government bodies and indicate the level of risk they are prepared to accept in pursuing political priorities. Senior leaders, accounting officers and boards set the organisation's approach to risk and oversee major decisions, while Audit and Risk Assurance Committees provide independent advice and challenge to boards and accounting officers.

Figure 3

Roles and responsibilities for managing risks in government bodies

Responsibilities for managing risks are multi-faceted and involve a wide range of individuals, teams, and supporting bodies

Governance bodies: set direction, oversee risk and performance, and provide challenge and accountability

Board

- Setting the organisation's approach to risk management
- Leading the assessment and management of opportunity and risk
- Determining the amount of risk that the organisation is willing to seek or accept to achieve its objectives (risk appetite)
- Ensuring that there are clear roles and responsibilities for risk management
- Helping incorporate risk management into business plans

Audit and Risk Assurance Committee

- Understanding the organisation's risks
- Discussing policies and attitude to risk with the board to ensure effective communication and mutual understanding
- Reviewing and challenging the organisation's risk management framework
- Reviewing and challenging the effectiveness of the measures implemented to manage risks (controls)

First line: responsible for delivering objectives and managing risks as part of their daily work

Accounting officer

- Ensuring that opportunities for debate, human resources policies and leadership foster the desired risk culture
- Monitoring the quality of the information received to ensure it supports effective decision-making
- Allocating appropriate resources to risk management
- Establishing risk management activities which cover all types of risks and processes across the organisation
- Demonstrating leadership and commitment to risk management by developing and communicating a policy to the organisation

Managers

- Have primary ownership, responsibility and accountability for identifying, assessing and managing risks

Operational staff

- Remaining alert to any risks
- Escalating risks and speaking out about them if deemed to be significant to ensure that other lines are aware

Second line: functions that support, monitor, challenge and facilitate the first line's management of risk, such as the risk function, counter-fraud, and some business continuity activities

Within these, the risk function is responsible for:

- Monitoring and facilitating effective risk management practices
- Monitoring compliance with risk management policies
- Assessing the effectiveness of the organisation's risk management
- Identifying emerging and evolving risks, and alerting senior management and governance bodies where appropriate

Third line: internal audit

- Evaluating the adequacy and effectiveness of governance, risk management and controls
- Advising on control strategies and the design of controls
- Providing assurance over the management of risks affecting the organisation
- Supporting sharing of good practice between organisations
- Advising on areas requiring improvement to ensure that risks are reduced or taken as appropriate

Figure 3 *continued*
Roles and responsibilities for managing risks in government bodies

Notes

1 Many government bodies adopt the 'three lines' approach, which allocates responsibility for managing risks (first line), supporting, monitoring and challenging risk management (second line), and providing assurance that risks are managed effectively (third line) to different parts of the organisation.

2 Supporting organisations, which provide guidance, capability-building, assurance and oversight to help organisations manage risks, include the Risk Centre of Excellence and Risk Profession, the Government Internal Audit Agency, the Cabinet Office, government functions, the National Infrastructure and Service Transformation Authority, and the Government Office for Science.

Source: National Audit Office analysis of guidance on risk management

1.3 Arm's-length bodies (ALBs) are responsible for managing their own risks, while their parent departments remain accountable to Parliament for ALBs' performance and stewardship of public funds. Departments and their ALBs are expected to have a shared understanding of risk, align their processes and risk appetite (the amount of risk they are willing to seek or accept), and monitor, report and escalate risks proportionately and promptly.

1.4 The Risk Centre of Excellence (CoE) – based in HM Treasury but filling a cross-government role – works to strengthen the risk management capability and credibility of risk professionals, staff outside the risk profession and senior leaders. It maintains and develops training, tools and guidance for risk professionals and wider civil servants, provides tailored support to individual organisations and the centre of government, and promotes knowledge-sharing and collaboration. Other cross-government bodies, such as the Cabinet Office, the National Infrastructure and Service Transformation Authority and government functions, support organisations to prepare for national risks and to manage risks in specialist areas such as project delivery.

Risk guidance, frameworks and tools

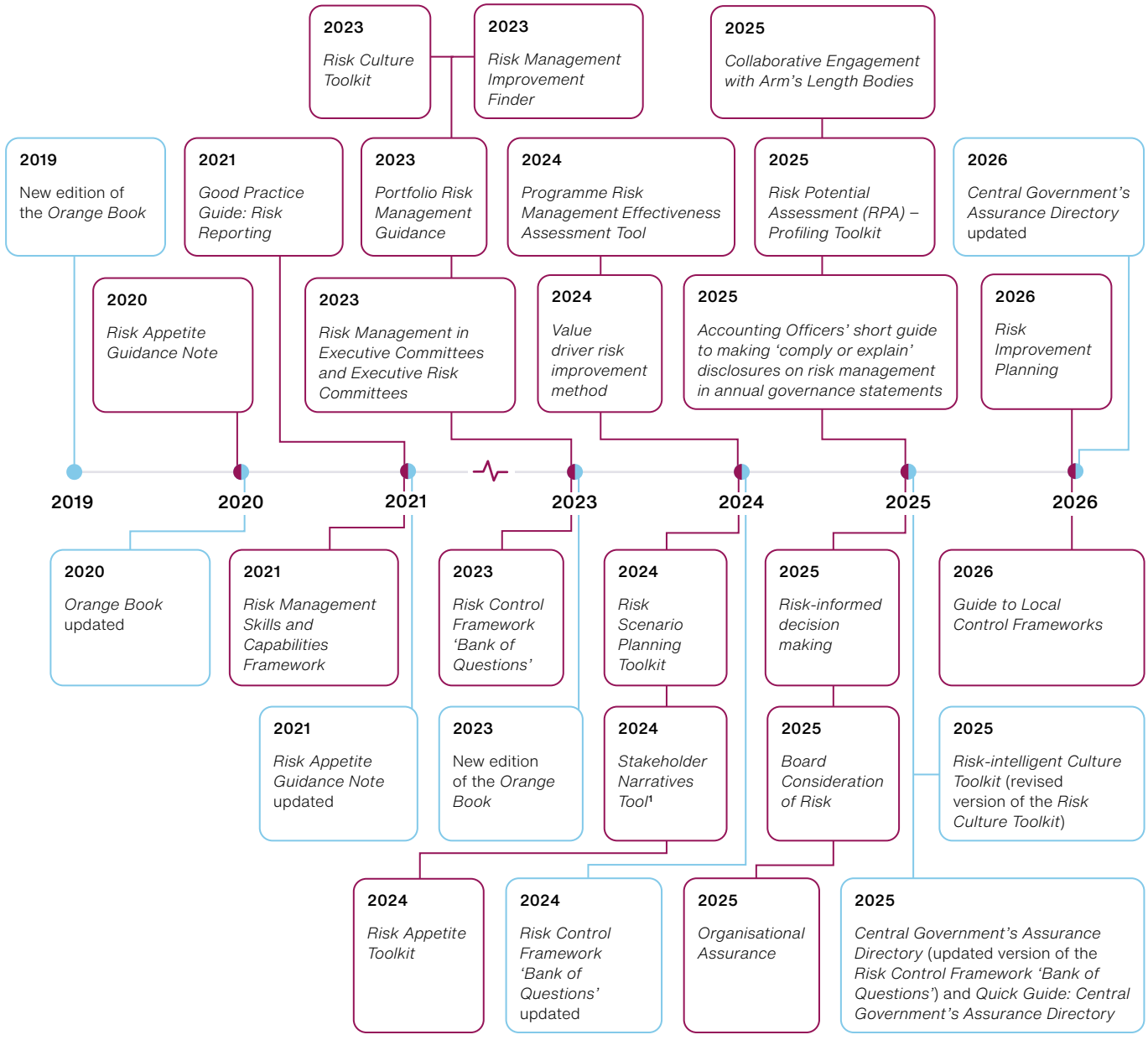
1.5 The government has strengthened its risk management guidance in recent years. It now has a well-developed set of principles, requirements and guidance to help departments and ALBs manage risks. This includes significant changes since 2019 to the *Orange Book* on managing risks in government and extensive guidance published after, both on specific aspects of risk management and as part of wider guidance covering activities such as crisis management, digital delivery, project delivery and options appraisal (**Figure 4**). All government departments are required to comply with the principles set out in the *Orange Book*, the *Corporate governance code in central government departments* and the functional standards, or explain why they have not.[2] Several voluntarily aim to comply with other risk management standards, such as ISO 31000 *Risk management*.

2 The functional standards set out what government bodies need to do to achieve consistent and efficient delivery of policy, outcomes and services in areas such as counter fraud, communications and finance.

Figure 4

New or updated risk management guidance for UK government bodies, 2019 to 2026

The government has issued a wide range of risk management guidance, at an increased rate since 2023



Notes

1 The *Stakeholder Narratives Tool* was first published in January 2024 and updated in July 2024.

2 Alongside risk management guidance, the government has revised the treatment of risk in guidance and standards on managing public money, business cases, options appraisal and digital delivery. It has also published new guidance on crisis management and project delivery, both of which include sections on managing risks. The government has expanded training and learning resources to help implement risk management guidance and build capability.

Source: National Audit Office analysis of UK government guidance

1.6 Risk professionals across government find the central resources valuable. Of the 62 respondents to our survey of risk professionals in central government departments and ALBs who answered this question, 98% engaged with tools and guidance provided by the Risk CoE, and 84% agreed that the Risk CoE's work has been useful. They would also welcome more support to identify, assess and manage opportunities. Greater focus on opportunities could help improve risk professionals' influence across organisations, and support the government's efforts to be less risk averse and take more well-managed risks.

> **A risk practitioner told us:**
>
> We only talk about risks when things are going badly, as opposed to focusing on opportunities. Management of opportunities is not really embedded.

Progress in adopting good practice across government

1.7 Our review of the risk frameworks and guidance of four case study bodies found they largely align with the government's good practice guidance.[3] For example, each organisation clearly sets out roles and responsibilities for risk management, covers both threats and opportunities, links risk management to the organisation's objectives and sets out its understanding of risk appetite. This is consistent with departments' assessments of their own compliance with the government's expectations for risk management.

1.8 Many government bodies have moved from tracking risks manually to risk management information systems. These digital systems bring risk information together, track mitigating actions, and show managers where follow-up is needed. While spreadsheets and other manual approaches can support effective risk management, particularly in smaller or less complex settings, they can require greater effort to maintain and update than dedicated risk management systems. Risk management information systems can improve oversight by highlighting overdue actions and giving senior leaders clearer information to scrutinise how risks are managed. However, such software still relies on staff consistently entering accurate information. Government bodies are at different stages in realising the benefits of risk management information systems. Some have started realising them, including the UK Hydrographic Office (**Example A**) and HM Revenue & Customs, while others have only recently made the transition or continue to rely on spreadsheets. As at September 2026, approximately a third of the 17 main government departments were tracking their risks manually.

3 Our case study approach is set out in Appendix One.

Example A

UK Hydrographic Office: risk dashboard



Background: The UK Hydrographic Office specialises in maritime geospatial data. It manages risks relating to its revenue-generating activities such as emerging competition, alongside its commitments to the UK government.



Approach: The UK Hydrographic Office developed an in-house risk register and dashboard based on user research. The risk register provides individualised views to help risk owners manage their risks and mitigations effectively. The dashboard presents risk information clearly and is accessible across the organisation. It supports a standing agenda item at monthly divisional management and executive leadership meetings.



Benefits: The dashboard has improved senior managers' understanding of risk. The previous risk reporting led managers to focus on a small set of strategic and corporate risks. The dashboard allows them to better understand the organisation's risk position at all levels and how well risks are being managed.

The dashboard also allows senior leaders to monitor whether risk information is up to date and whether mitigating actions are overdue, and to follow up with individuals and teams. The number of overdue actions reduced significantly after the dashboard was introduced.

1.9 Despite progress across government, departments and ALBs vary in how far they implement the government's risk management principles, requirements and guidance. The following paragraphs illustrate examples relating to options appraisal, the information used to anticipate and respond to risks, and assurance over how well risks are being managed.

1.10 In 2025, the government updated its guidance on ensuring value for money when using public resources to clarify how decision-makers should take account of risk and uncertainty. The guidance requires decision-makers to consider the chances of different degrees of success and failure when assessing options. This process aims to support a more realistic assessment of uncertainty, enable better comparison of options, and help identify the option most likely to deliver value for money. Government bodies have not yet adopted this approach consistently. The Ministry of Defence told us it applies it proportionately, with higher-value projects subject to greater scrutiny of cost, duration, risks and mitigations before the final decision is made.

1.11 Government bodies are not yet making full use of performance information and early warning indicators to anticipate and monitor risks, limiting the quality of risk reporting and the speed of response. For example, organisations could use employee satisfaction scores and sickness rates as early warning indicators that prompt action to reduce the risk of staff turnover. While many organisations use quantitative measures to monitor progress against their objectives, we found limited use of indicators to provide early warning of increasing risks and prompt action. Reporting of principal risks to senior decision-makers is often qualitative, even when quantitative information could help. Some organisations have started work to link risks to performance indicators. For example, the Ministry of Justice uses metrics in its reporting to senior committees to set out changes in risks and the progress made in bringing them to a tolerable level.

1.12 Many government bodies do not know, with confidence, whether risks are being managed effectively and efficiently across the organisation. Government guidance recommends using assurance maps to show which teams or controls provide assurance over key risks, business areas or business processes, and the strength of the assurance provided (**Example B**). Most departments assessed themselves as having at least partially established an approach to assurance in 2024-25, and 74% of 62 respondents to our survey said they used assurance mapping. However, our fieldwork and the Government Internal Audit Agency's work found several organisations that did not have assurance maps or whose maps were still being developed. Poorly designed assurance arrangements can also be ineffective. An independent review of the High Speed Two programme to deliver a new railway between London and Birmingham found that fragmented assurance arrangements led to duplication, inconsistencies and delays.[4]

Capacity and skills

1.13 Central risk teams are often small relative to the size, complexity and risk profile of the organisations they support. In our survey, 66% of 62 respondents said they had fewer than seven full-time equivalent (FTE) staff in their central risk team, while 37% reported having one to three FTE staff. This includes large organisations where small central risk teams are responsible for overseeing a broad range of risk areas. For example, the central risk team of the Government Property Agency, which manages most of the government's office portfolio, consisted of one employee as of August 2026. Some risk professionals told us limited capacity meant they had to deprioritise certain activities, such as engaging with operational teams, and that smaller teams could be less resilient to staff turnover and absences.

4 James Stewart, *Stewart Review: Major Transport Projects Governance and Assurance Review: The HS2 Experience*, June 2025.

Example B

NHS Blood and Transplant (NHSBT): assurance mapping



Background: NHSBT works to ensure that patients receive the blood and organ donations they need. NHSBT developed an assurance map over the last two years.



Approach: Directorates identified their key business processes, and directors assessed the quality of risk management for each process using the following criteria.

- Governance: what oversight, policies and independent checks are there for each process?
- Application: how well is the process done, and are there complaints or quality incidents?
- Compliance: are statutes and regulations being complied with?

NHSBT carries out quarterly updates and annual reviews including challenge meetings with executive directors. It gathers information from existing sources, including its risk management system, and produces a live dashboard for senior leaders.



Benefits: NHSBT can manage actions to strengthen assurance across the organisation, give confidence to its board that risks are managed properly, show compliance with legal requirements, and otherwise minimise burdens for staff.

1.14 However, most risk professionals we spoke to did not see increasing team size and capability as a priority. Of the 62 risk professionals who responded to our survey question on skills, 84% said their team has adequate skills and expertise to support effective decision-making. While there is variation in risk capability between organisations, risk professionals told us that improving risk capability across their organisation is a higher priority than increasing resources or expertise within central risk teams. They emphasised that effective risk management depends on risk being integrated into day-to-day operations, rather than being the responsibility of a central team alone. (We cover culture, leadership and influence in Part Two.)

1.15 To support this, central risk teams have sought to strengthen risk awareness across their organisations by:

- delivering tailored training for staff in specific roles, such as those preparing reports for governance committees, alongside all-staff events. The Ministry of Justice's 2025 Risk Awareness Week recorded nearly 900 attendances across its events and included training, keynote speeches and risk-themed escape rooms;
- appointing members of the central risk team as risk 'business partners' for individual business areas; and
- establishing networks of 'risk champions' – members of operational teams who help colleagues identify, assess and escalate risks, and act as links with the central risk team.

A risk practitioner told us:

> Our risk team is small, but it relies on other people across the business, using a 'hub and spoke' model. The team has trained at least one person in each directorate and relies on their ability to identify and flag issues. This arrangement works well.

1.16 Organisations do not consistently identify and plan for future risk resourcing needs, which may reduce their effectiveness over time. For example, increased use of artificial intelligence (AI) tools could reduce some routine tasks, while requiring different skills to oversee AI-enabled processes. Views from risk professionals were mixed on whether organisations had clear and credible plans to address gaps in the risk team's resourcing and skills, with 48% of 62 respondents to our survey question agreeing that such plans were in place, and 44% disagreeing. We found limited evidence that central risk teams routinely assess current and future workforce requirements. In previous reports, we found that this can undermine effective workforce planning.[5] Risk teams should consider how future changes in demand, technology and ways of working may affect the capacity and skills they require, and use this to inform long-term workforce planning.

5 For example, Comptroller and Auditor General, *Lessons learned: the government's use of external consultants*, Session 2024–2026, HC 1381, National Audit Office, November 2025; Comptroller and Auditor General, *Government workforce planning – lessons learned*, Session 2026-27, HC 267, National Audit Office, July 2026.

Part Two

Culture, leadership and influence

2.1 An organisation's risk culture reflects how its people think about and respond to risk. A positive risk culture encourages informed risk-taking, collaboration and open discussion of concerns, so risks can be managed effectively and lessons can be learned. Senior leaders can support this by setting the right tone and creating an environment where people feel safe to raise concerns. Where risk culture is strong, risk professionals are more likely to be involved early in important decisions, helping shape options and inform trade-offs rather than providing assurance after decisions have been made.

2.2 This part covers:

- risk culture;
- leadership of risk management;
- risk professionals' influence on decisions;
- how promptly risks are identified and escalated; and
- oversight and governance of risk.

Culture

2.3 Our past work has highlighted how setting a positive risk culture is critical to the successful delivery of government programmes and services. The Bank of England's 'no surprises' culture was important to its successful modernisation of the Real-Time Gross Settlement system (**Example C** overleaf). By contrast, the Public Accounts Committee found that National Savings & Investments' 'positive news' culture meant it did not learn lessons. This affected its ability to deliver its digital business transformation programme, which was significantly delayed and over budget.[6]

6 Committee of Public Accounts, *NS&I's transformation programme*, Sixty-seventh Report of Session 2024-26, HC 1237, February 2026.

Example C

Bank of England: risk culture



Background: The Bank of England delivered a programme to modernise the system that settles high-value payments between parties in the UK, which is part of the UK's critical national infrastructure. It successfully launched the new system in April 2025.



Approach: The programme fostered a transparent 'no surprises' culture, with strong leadership and collaborative working between business and technical areas. The Bank created a behaviour manifesto setting out expectations for staff. It established several routes for staff to voice opinions, including an anonymous channel for raising concerns, and ran events to allow staff to highlight issues. These included weekly drop-ins and town hall events.

Senior leaders reinforced a team culture of everyone playing their part, for example by attending weekend dress rehearsals for the launch of the new system.

To avoid siloed working, business and technology specialists worked from the same location, and programme roles had representation from both Bank staff and the external delivery partner.



Benefits: The Bank's approach managed risks effectively and addressed several common problems we have seen in the government's digital transformation programmes. The Bank told us that building the right culture was an important enabler of delivery. It strengthened collaboration between teams, reducing silos and fostering a shared sense of ownership and accountability for delivery.

2.4 Government bodies are expected to regularly assess their risk culture, but this is not consistently done. Three of our four case study organisations made progress in assessing their risk cultures. For instance, the then Department for Science, Innovation & Technology (DSIT) reviewed the perspectives of staff on risk across its directorates. This demonstrated that teams who originated in different parts of the government prior to joining DSIT had substantially different risk cultures. DSIT used this to identify actions to improve culture in specific groups of staff, such as through dedicated training and support on using risk appetite and frameworks, or appointing risk champions within teams.

2.5 Staff confidence in speaking up about risks has strengthened since 2017, but variation between organisations indicates that risk culture remains uneven across government. Of the 62 respondents to our survey of risk professionals in central government, 71% said their organisation has a healthy culture that enables risks to be discussed openly and honestly. The Civil Service People Survey provides insight into civil servants' confidence in speaking up when they identify a policy or delivery risk. From 2017 to 2021, the median score for this question increased from 66% to 75%, and it has remained broadly stable since. Variation between organisations has reduced since 2017, but substantial differences remain (**Figure 5** overleaf).

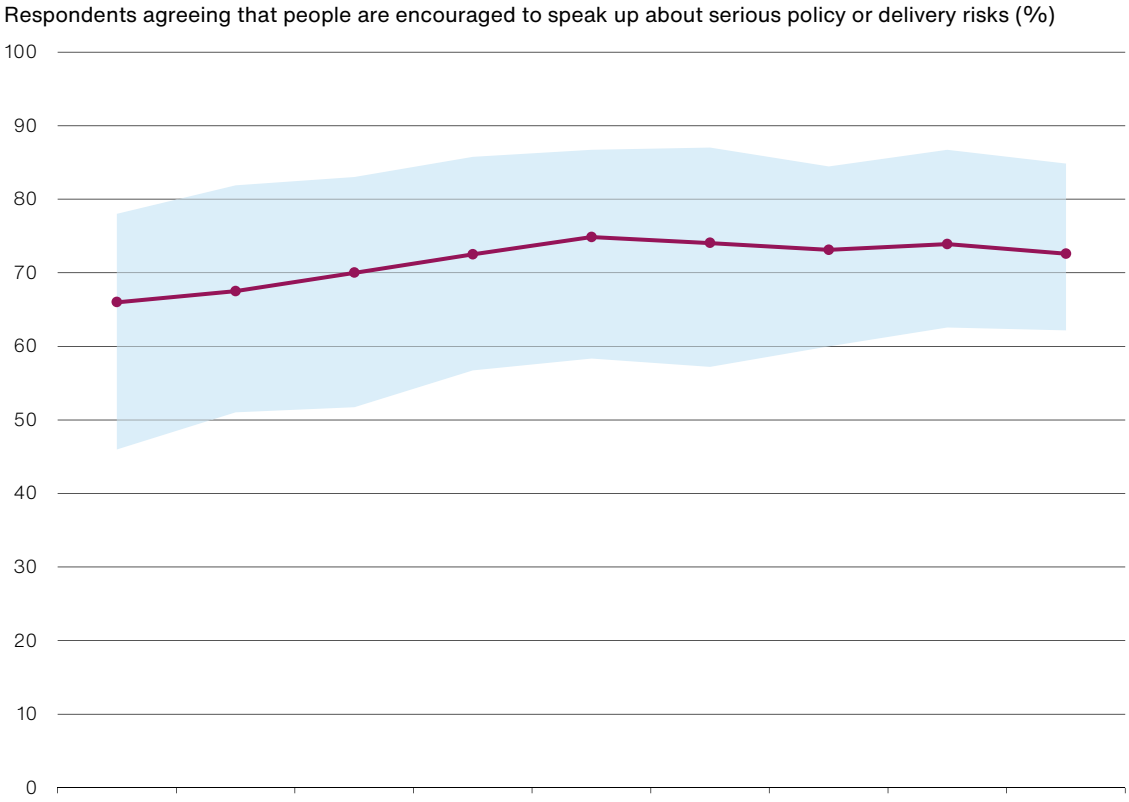
Leadership

2.6 Senior leaders play an essential role in shaping a positive risk culture. By demonstrating the value of risk management, encouraging open discussion and promoting proportionate risk-taking, leaders can help ensure that decisions take account of risk and support improvement, innovation and the effective delivery of public services. The government sets out these leadership behaviours in its Civil Service Success Profiles and requires senior leaders to apply them in the Performance Management Framework for the Senior Civil Service. The government intends to withdraw the Success Profiles, and to introduce a new Civil Service Leadership Standard.

Figure 5

Civil servants' views on whether they are encouraged to speak up when they identify serious policy or delivery risks, 2017 to 2025

In response to the annual Civil Service People Survey, officials have broadly reported feeling able to raise concerns, with median scores improving slightly since 2017 and variation between organisations narrowing over time



	2017	2018	2019	2020	2021	2022	2023	2024	2025
Median score	66	68	70	73	75	74	73	74	73
95th percentile	78	82	83	86	87	87	84	87	85
5th percentile	46	51	52	57	58	57	60	63	62
Range (5th to 95th percentile, percentage points)[1]	32	31	31	29	28	30	24	24	23

Notes

1 Ranges were calculated before rounding and may therefore differ from those calculated using the rounded percentages shown.

2 Percentage of respondents to the Civil Service People Survey, 2017 to 2025, who answered 'agree' or 'strongly agree' to the statement: "In [my organisation], people are encouraged to speak up when they identify a serious policy or delivery risk."

3 The median is the score where half of the surveyed organisations scored higher and half scored lower. The range shown covers the middle 90% of organisation scores each year, excluding the lowest and highest 5%.

4 Scores were calculated using the full set of government bodies included in the Civil Service People Survey dataset for each year.

Source: National Audit Office analysis of data from the Civil Service People Survey, available at: https://www.gov.uk/government/collections/civil-service-people-surveys

2.7 We observed examples of senior leaders supporting effective risk management. Risk professionals told us that leaders in their organisations encourage ownership of risks across management teams and consider risks when making decisions. In several organisations, changes in leadership led to improvements in organisational attitudes towards risk management and the priority it received (**Example D**). Our survey also generally indicated positive leadership behaviours. Out of 62 respondents, 73% agreed that senior leaders in their organisations actively engage with risks rather than treat risk management as a compliance exercise, and 82% perceived senior leaders to actively promote well-managed risk-taking (**Figure 6** overleaf).

Example D

Home Office: setting the tone at the top



Background: Following previous concerns about the effectiveness of risk management, the Home Office's leadership prioritised improving risk management across the department.



Approach: The leadership identified room for improvement in the Home Office's approach to risk management and made improving risk and assurance a priority. Senior leaders were asked to identify specific actions to improve risk management in their areas. The Permanent Secretary introduced a process for holding directors general to account, including on whether risks were managed appropriately. The Executive Committee introduced regular, extended discussions of risk. Regular sessions were also introduced, led by directors general, to strengthen challenge and oversight of key risks.



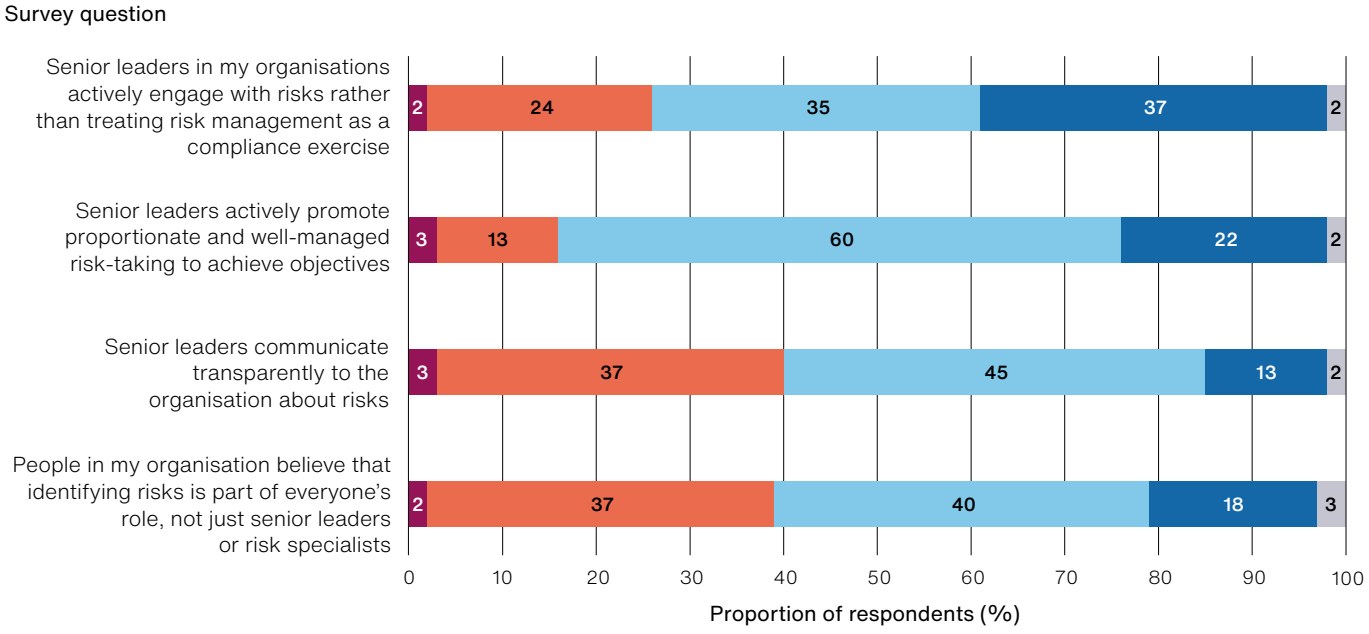
Benefits: The Home Office reports that these changes raised the profile of risk management across the organisation, enabled greater challenge and oversight of significant risks, and supported meaningful discussions with ministers about risk appetite, delivery trade-offs and what could realistically be achieved.

2.8 However, senior leaders' engagement with risk management as a key element in effective decision-making remains inconsistent across government, which can mean organisations are more exposed to risks, or miss opportunities to improve services. While we observed examples of good risk leadership, risk and governance professionals told us some leaders do not view risk management as enabling informed decision-making and give it limited priority in governance forums. In our survey, 40% of 62 respondents told us that senior leaders do not communicate transparently to the organisation about risks. Although organisations include major cyber risks in their risk registers, leaders do not always understand these risks or recognise how they relate to their strategic objectives. This can reduce the use of risk information to support decisions, leaving organisations exposed to incidents.

Figure 6

Risk professionals' perceptions of senior leaders' engagement with risk management, April to June 2026

Survey responses suggest generally positive perceptions of risk leadership, with only some areas for improvement



Notes

1 Respondents to our survey answered the following question: "Based on your experience as a risk professional, to what extent do you agree with the following statements?"

2 In total, 62 risk professionals from across government responded to this survey question.

Source: National Audit Office analysis of responses to our survey of risk professionals across government

2.9 Several factors limit senior leaders' engagement with risk management. These include insufficient understanding of the value of risk management and of leaders' responsibilities for managing risks; a perception that risk management hinders delivery, rather than supports it; and overly technical risk reporting that is not focused on decision-makers' needs. Risk, assurance and governance professionals told us that, in some organisations, leaders focus on delivering objectives without sufficient attention to the risks that affect successful delivery and to concerns raised through risk processes. Targeted risk training and induction for senior civil servants, alongside more accessible, decision-focused reporting, can improve their engagement with risk management.

> **A risk practitioner told us:**
>
> The biggest change came when we moved away from technical risk detail and used a simple picture and storyline to show where risks were heading, and the confidence behind those trends. This helped senior leaders have a more meaningful conversation and reach decisions, rather than being presented with a list of risks and moving on.

Influence of risk professionals

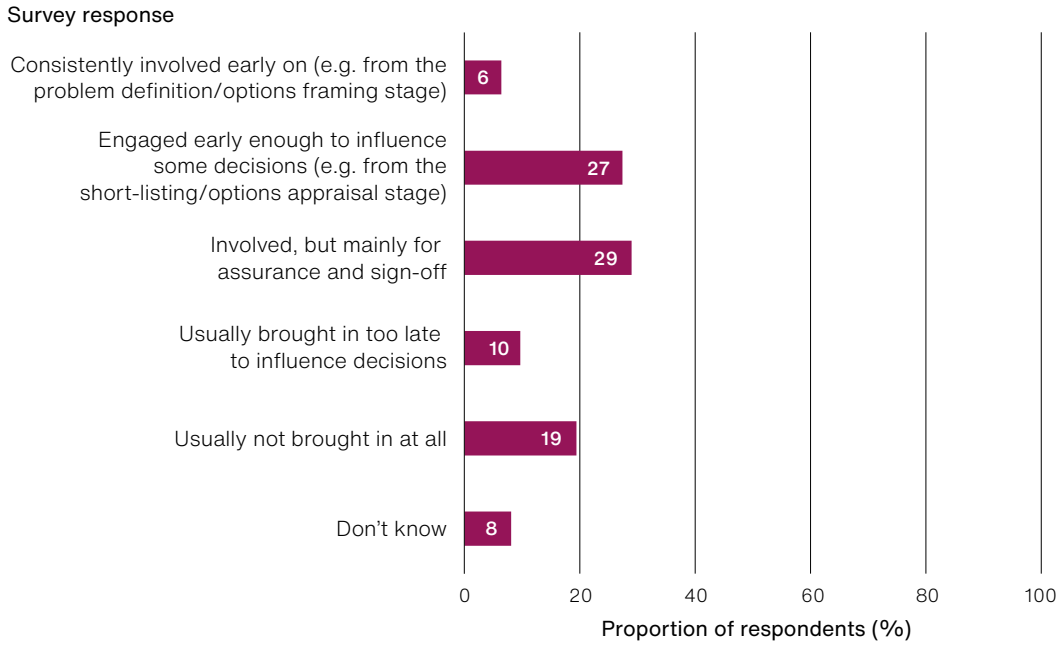
2.10 Risk professionals add most value when they are involved early enough to shape decisions. They can help organisations understand uncertainty, assess threats and opportunities, and challenge optimistic assumptions. Risk experts should be involved when options, priorities and trade-offs are being considered, rather than be consulted at the end of this process.

2.11 Risk professionals across government do not have enough influence over major decisions. In our survey, 58% of 62 respondents said risk professionals are typically brought in either too late to shape decisions, mainly to provide assurance and sign-off, or not at all (**Figure 7** overleaf). Risk professionals also told us that their input and challenge are acted on inconsistently. Conversations often happen at leadership level without involving the risk team. We found limited evidence of major decisions or organisational direction changing because of input from risk professionals. Some risk teams are increasing their influence by focusing discussions on the intended outcomes and benefits, rather than purely on threats, building stronger relationships with delivery functions, and proactively working to engage earlier in planning and change processes.

Figure 7

Involvement of government's risk professionals in decision-making, April to June 2026

Over half (58%) of risk professionals responding to our survey told us they were involved too late to influence major decisions, primarily for assurance and sign-off, or not at all



Notes

1 Respondents to our survey answered the following question: "At what stage are risk professionals typically involved in major decisions?"

2 In total, 62 risk professionals from across government responded to this survey question.

Source: National Audit Office analysis of responses to our survey of risk professionals across government

2.12 In hierarchical organisations, low seniority or status of those leading risk teams can restrict their access to senior decision-making forums, reducing their ability to influence decisions and raise the profile of risk management. Nearly half (45%) of 62 survey respondents said the most senior person responsible for monitoring and overseeing risk management in their organisation was below the senior civil service level.

2.13 More departments now have a Chief Risk Officer (CRO), but risk professionals offered mixed views on whether this helps increase the influence of risk teams. The number of CROs in central government departments has increased significantly in the past 10 years. We found evidence of four CROs being in post in 2016. Eleven CROs were in post in June 2026. As senior risk leaders, CROs can help boards and executive teams understand uncertainty, take account of risk and weigh risks against opportunities. Risk professionals told us that, while a CRO can raise the visibility and influence of risk management, the title matters less than having an experienced leader who ensures that risk is considered before decisions are made. Given the range of factors that influence risk management effectiveness, our evidence did not allow us to identify a consistent relationship between the presence of a CRO and how effectively risks are managed.

> **A risk practitioner told us:**
>
> Every organisation needs a 'critical friend' – someone close to senior leadership. This could be the chair of the Audit Committee, the Finance Director or another senior individual. There needs to be someone who is willing to put their hand up and say, 'Wait, have we thought about this?'

2.14 In contrast to the often limited influence of risk professionals across government, the Risk Centre of Excellence (CoE) told us it is increasingly able to support decision-making at the centre of government. It has developed risk assessments for government priorities and supported cross-government taskforces, including work on sharing police data with probation services. The Risk CoE sees this as evidence of progress in making risk a routine part of decision-making. It considers that organisations can support this by starting with their intended outcomes and identifying the risk management activities that will best support them.

Risk identification and escalation

2.15 Government guidance sets a clear expectation that staff at all grades, as well as ministers, play a role in managing risks, and that managers and staff in specialist roles should manage risks proactively. To support this, the Risk CoE has developed risk training and learning resources for non-risk professionals, including ministers and senior civil servants. The Risk CoE works with government functions to strengthen the risk management capability of those in specialist roles, including by updating guidance to strengthen consideration of risk in areas such as crisis management and digital delivery. It contributed to the *Teal Book* on project delivery, is supporting updates to training for senior project delivery professionals, and is piloting training for senior leaders responsible for major projects.

2.16 Despite an improving culture of raising concerns across government (paragraph 2.5), key risks are not always mitigated or escalated promptly. Our survey suggests that risk identification and escalation are widely established across operational teams, with 85% of 62 respondents agreeing that first-line teams routinely identify, monitor and escalate risks. However, only 58% said people in their organisations view identifying risk as everyone's role. Government Finance Function data indicate that finance staff often have only a basic understanding of risk and make minimal use of it in their role. Risk professionals told us the effectiveness of those in charge of risks in the first line is variable. Several government bodies have significant backlogs of outstanding mitigating actions, indicating that risks are not always addressed promptly. Reasons can include risk management being treated as a compliance exercise, a 'good news' culture that discourages open discussion and escalation of risks, and delivery pressures that can cause risk management activity to be deprioritised.

Oversight and governance

2.17 Audit and Risk Assurance Committees (ARACs) provide independent advice and challenge to the board and accounting officer to help ensure organisations understand key risks and respond appropriately to them. By monitoring risk culture and reviewing how well risk appetite is understood across the organisation, ARACs can provide assurance that organisations take well-managed risks to support innovation and improvement. Of the 62 respondents to our survey, 87% agreed that the board and ARAC provide meaningful challenge to ensure key risks are managed effectively.

2.18 However, ARACs often lack the expertise needed to challenge management effectively on emerging risk areas such as cyber security, digital transformation, artificial intelligence and climate change. The Risk CoE also expressed concern about whether there is sufficient risk management expertise in ARACs across government. Without sufficient expertise, ARACs may be less able to test whether management is doing enough to address key risks. Smaller bodies, in particular, may have less access to specialist skills. ARACs can address this by drawing on experts within the department and its arm's-length bodies (ALBs), while recognising these experts are not independent. For example, DSIT provided training on cyber security and environmental disclosures to the chairs of its ALBs' ARACs.

Part Three

Using risk management to inform decision-making in practice

3.1 Effective risk management helps organisations make better decisions, manage trade-offs and respond to uncertainty. This part examines how government bodies use risk management to inform decision-making in practice, by considering how they:

- identify and respond to emerging and evolving risks;
- define and apply risk appetite (the amount of risk they are willing to seek or accept);
- manage risks that cut across organisational boundaries; and
- learn and improve how they manage risks.

Identifying and responding to emerging and evolving risks

3.2 Anticipating future risks helps organisations prepare for shocks, respond to change, and make decisions that account for short- and long-term impacts. Organisations should monitor emerging trends, draw on expertise, use techniques such as horizon scanning and scenario analysis, and test plans against plausible scenarios.

3.3 Many organisations use horizon scanning and scenario planning to anticipate issues, and some focus on the long-term trends that might affect their ability to deliver services. Of the 62 respondents to our survey of risk professionals in central government, 92% said their organisation uses horizon scanning or scenario planning to manage risks. We observed good examples of these techniques being used to anticipate future challenges and opportunities. For example, the Ministry of Justice has assessed the civil emergency risks most likely to materialise over the next six months and analysed global long-term trends that may affect it over the next five to fifteen years.

3.4 However, timely action in response to emerging and evolving risks is inconsistent and often lacking. For example, following the emergency evacuation from Afghanistan in 2021, the Ministry of Defence (MoD) supported the relocation of Afghan citizens at risk due to their links with the UK. The House of Commons Defence Committee found that, during this emergency phase, the MoD prioritised speed over developing robust data handling systems. Once the crisis had passed, the MoD did not formally assess whether its approach remained appropriate. This contributed to significant data security breaches involving more than 18,500 applications.[7]

Risk appetite

3.5 Risk appetite is the amount of risk an organisation is willing to seek or accept in pursuit of its objectives. For example, an organisation with a higher risk appetite for service improvement may accept short-term disruption when trialling a new digital process, but it may set a low appetite for fraud risk by requiring additional checks before payments are made. A clear risk appetite helps organisations make deliberate choices about the risks they are willing to accept to achieve their objectives. It supports trade-offs between competing priorities. It gives staff confidence to test new approaches and improve services in areas where the organisation is prepared to accept greater risk (**Examples E and F**), whereas uncertainty about what risks are acceptable can inhibit innovation.

3.6 While government bodies are increasingly articulating their risk appetite, this does not yet consistently translate into clear or effective action. Several government bodies are introducing or revising risk appetite statements and guidance, including accepting greater risk to improve and innovate. However, only 47% of 62 respondents to our survey said their organisation uses risk appetite to inform decisions, and only 36% said that, when a decision exceeds risk appetite, the rationale and trade-offs are documented. Our recent reports have found similar gaps, with the Department for Environment, Food & Rural Affairs only beginning to integrate risk appetite into resourcing decisions and the Department for Transport not clearly setting out its risk appetite for innovation to guide investment decisions.[8]

7 House of Commons Defence Committee, *Shifting heaven and earth? The Afghan data breach and resettlement schemes*, First Report of Session 2026-27, HC 69, July 2026.

8 Comptroller and Auditor General, *Resilience to animal diseases*, Session 2024-25, HC 946, National Audit Office, June 2025; Comptroller and Auditor General, *Innovation in transport*, Session 2026-27, HC 20, National Audit Office, May 2026.

Example E

HM Revenue & Customs (HMRC): making informed trade-offs to achieve strategic objectives



Background: The COVID-19 pandemic and associated public health restrictions created a risk of widespread business failure and job losses. HM Treasury and HMRC responded by introducing the Coronavirus Job Retention Scheme and the Self-Employment Income Support Scheme.



Approach: The government aimed to provide financial support quickly to protect jobs. To enable rapid delivery, the government streamlined some controls and approvals, consciously accepting a higher risk of fraud and error than normal. Although these decisions were not always framed in terms of risk appetite, they reflected a deliberate trade-off between speed and risk exposure.



Benefits: The schemes were launched quickly and ahead of schedule, were straightforward to access, and helped protect jobs. While their speed and scale increased the risk of significant levels of fraud and error, HMRC kept the resulting fraud and error risks under review. As it better understood their nature and scale, it introduced additional upfront controls and post-payment checks to reduce losses.

Example F

Department for Work & Pensions (DWP): using risk appetite to accelerate progress and maintain momentum



Background: Child maintenance payments are financial contributions made by a parent who does not live with their child. DWP estimates that around 8,000 child maintenance cases each month experience an unplanned breakdown in payments, disrupting support for children.



Approach: DWP developed a model that predicts the probability of a breakdown and explains the factors behind the prediction. This allows DWP teams to deliver tailored interventions to improve compliance rates. Officials told us a higher risk appetite for innovation during the COVID-19 pandemic helped accelerate progress and maintain momentum.



Benefits: Since becoming operational in March 2024, DWP's model has helped prevent an estimated 715 cases a month from falling into arrears. It has also released capacity equivalent to 49 full-time roles, enabling officials to focus on other priorities.

3.7 In June 2026, most central government departments reported that the majority of their principal risks were outside their stated risk appetite or tolerance, often for multiple years.[9] Principal risks may have been escalated precisely because they exceeded appetite, and organisations may decide to tolerate them after considering the trade-offs. However, persistent differences between an organisation's stated appetite and actual exposure may indicate that its risk appetite does not accurately reflect the level of risk it is prepared to accept, or that actions to bring risks within appetite are ineffective or constrained. For example, reliance on legacy technology and difficulties recruiting and retaining specialist cyber staff may constrain departments' ability to bring cyber security risks within appetite. Some officials told us that funding constraints made addressing persistent risks challenging, while legal or regulatory constraints mean organisations do not have complete discretion to set their appetite for certain risks. Others reflected that formally increasing appetite could be seen as accepting serious harm, such as casualties, or may give the misleading impression that no further action is needed to manage the risk.

Managing risks that cut across organisational boundaries

3.8 The government faces many risks that span organisational boundaries, including arm's-length bodies (ALBs), suppliers, other departments and local government. Responsibilities, dependencies and controls are often shared across different bodies. We have previously highlighted how effective coordination, clear accountability and robust governance are essential to ensure cross-cutting risks are identified and managed collectively, rather than falling between organisational responsibilities.[10] This will become increasingly important as central government transfers more responsibilities to local and regional government.

9 Departments varied in whether they monitored principal risks against risk appetite (the amount of risk they are willing to seek or accept), risk tolerance (a related measure used to define tolerable levels of risk), both, or neither. Some departments also changed how they monitored and reported principal risks over time.

10 Comptroller and Auditor General, *Lessons learned: Cross-government working,* Session 2022-23, HC 1659, National Audit Office, July 2023.

3.9 Our past work has found that government bodies often have a limited understanding of how risks interact and how issues in one area can affect others. For example, we reported in 2026 that the Cabinet Office's programme to roll out shared back-office services across government did not adequately consider how risks could compound. Weaknesses in tracking interdependencies with other programmes affected planning and delivery.[11] Use of techniques such as interdependency mapping remains variable, with 31% of 62 respondents to our survey saying they use it to manage risks. We did, however, identify some good practice examples. National Highways developed a matrix of interdependencies among its principal risks. It told us that, when senior management identified a new risk relating to the operability of the strategic road network, the risk team used the matrix and an analysis of the causes and consequences of each risk to coordinate the response across the organisation, including the executive directors responsible for managing related risks. The Bank of England's Real-Time Gross Settlement system renewal programme managed complex and evolving risks and interdependencies, replanning where necessary in response to internal and external factors.[12]

3.10 Departments' oversight of ALB risks is inconsistent, limiting their ability to exercise proportionate oversight, challenge ALBs, support them before issues escalate, and understand how risks across organisations may compound and affect the outcomes for which the department is ultimately accountable. While some departments have improved how they integrate ALB risks into reporting and oversight, there is variation in how well departments understand their ALBs' risks, reflect them in reporting, communicate risk appetite to their ALBs, learn from and challenge them. The Government Internal Audit Agency found that departments often lack consistent arrangements to aggregate risks across their ALBs, define when risks should be escalated, and translate departmental risk appetite into guidance that ALBs can apply. Some ALBs' risk teams told us they had limited contact with their sponsoring department's risk team or were not made aware of the department's risk appetite, reducing both sides' ability to develop a shared view of risks and act before issues escalate. The Risk Centre of Excellence (CoE) has published guidance to help departments and ALBs develop effective relationships, promote a shared understanding of risk, and support proportionate monitoring and reporting.

11 Comptroller and Auditor General, *Update on government shared services*, Session 2024–2026, HC 1718, National Audit Office, March 2026.
12 Comptroller and Auditor General, *The Bank of England's Real-Time Gross Settlement system renewal programme*, Session 2024–2026, HC 1546, National Audit Office, December 2025.

3.11 Limited oversight of project, programme, delivery partner and supplier risks also hinders government bodies' ability to anticipate and respond to disruptions. For example, several government bodies have insufficient visibility of the risks their suppliers face, especially in fast-changing supply chains involving multiple suppliers or subcontractors. We reported in 2026 that HM Prisons and Probation Service had strengthened its oversight and worked with electronic monitoring suppliers to improve performance, but unclear system ownership and challenges in managing interdependencies between suppliers contributed to delays and inefficiencies.[13] Audit Wales has found similar issues, noting that Welsh local authorities often lack arrangements to ensure they take account of risks arising from partner organisations.

3.12 Many significant risks facing departments require cross-government collaboration, but those responsible for managing them often lack the authority, levers or incentives to do this in an integrated way. For example, the Department for Environment, Food & Rural Affairs leads the government's work on the resilience of food supply and engages directly with other government departments on specific dependencies, such as chemicals, that affect the food supply chain. Defra stated in 2025 it had "very little confidence" that cross-government governance of critical national infrastructure was sufficiently joined-up.[14] Officials told us collaboration works best when organisations have shared objectives, but these are not always in place. Following the COVID-19 pandemic, Parliamentary committees proposed creating a government-wide Chief Risk Officer role to support a more coordinated approach to managing risks.[15] While the government has not established this role, it took steps to strengthen risk management capabilities through the Government Risk Profession and Risk CoE.

13 Comptroller and Auditor General, *Electronic monitoring: improving resilience to meet increasing demand,* Session 2026-27, HC 266, National Audit Office, July 2026.
14 Comptroller and Auditor General, *Resilience of the food supply chain to disruptions*, Session 2026-27, HC 587, National Audit Office, September 2026.
15 House of Commons Committee of Public Accounts, *Government preparedness for the COVID-19 pandemic: lessons for government on risk*, Forty-Sixth Report of Session 2021-22, HC 952, March 2022; House of Lords Select Committee on Risk Assessment and Risk Planning, *Preparing for Extreme Risks: Building a Resilient Society*, Report of Session 2021-22, HL Paper 110, December 2021.

Learning and improvement

3.13 The government should continuously learn from successes and failures to improve delivery, efficiency and value for money. We found several examples of government bodies learning from experience to improve how they manage risks. For example, Sizewell C Ltd (the company responsible for delivering the Sizewell C nuclear power plant) and the Department for Energy Security & Net Zero used lessons from past mega-projects to develop new approaches to managing delivery risks. These include ensuring the company is free to move spending between years, and using contracting arrangements intended to encourage collaboration and risk-sharing.[16]

3.14 Many government bodies collect and review incidents and near misses in areas such as cyber security, data protection, and health and safety, to update and improve their approach. The UK Health Security Agency told us that it records between 800 and 1,000 health and safety incidents a year, allowing it to review cases, track their resolution, and identify common themes to inform future work.

3.15 The Risk CoE provides tools and guidance to help organisations improve how they manage risks. However, our survey of risk practitioners and the Government Internal Audit Agency's work found limited engagement with Risk CoE tools intended to help organisations strengthen their risk management improvement plans. Beyond its published guidance, the Risk CoE plays an important coordinating role across the government risk community. Groups such as the Heads of Risk Network meet regularly to share developments and good practice. They are well attended and valued by risk practitioners.

3.16 Government bodies do not routinely have robust, documented risk management improvement plans, making it harder to target improvement, monitor progress and sustain change. However, our fieldwork identified organisations taking a more structured approach to planning and implementing improvements. For example, in 2025 the then Department for Science, Innovation & Technology set an action plan that assessed the risk maturity of each division, set out targets for improvement for 2025 and 2026, and assigned improvement tasks to specific individuals.

3.17 No central body assesses how effectively government bodies manage risks overall to provide a consistent basis for identifying leading practice and areas for improvement across government. Government functions may assess how effectively organisations manage risks in specific areas. For example, the Government Grant Management Function coordinates continuous improvement assessments, sense-checks the results through assessments of specific grant schemes, reviews improvement plans, and supports organisations to strengthen their capability. The Risk CoE provides helpful improvement planning guidance and works to improve risk capability and skills across government. However, it is not responsible for monitoring continuous improvement in the area.

16 Comptroller and Auditor General, *Sizewell C*, Session 2026-27, HC 33, National Audit Office, May 2026.

3.18 Risk teams across government are beginning to use artificial intelligence (AI) to improve efficiency and support decision-making. The Risk CoE is piloting AI agents to assist with tasks such as horizon scanning, developing assurance maps and helping users apply risk guidance to policy areas. It also provides model instructions and guidance to help government organisations create their own AI agents.
The Rural Payments Agency is using AI tools to analyse large volumes of risk data, make the analysis accessible to non-risk professionals, and design visuals to present risk information to senior leaders.

A risk practitioner told us:

AI tools are collapsing iteration cycles: how quickly we can follow up on risk workshops, update risk information and challenge the underlying data. This gives us, as risk managers, more time to be the people in the room talking to senior leaders about the choices they face. That's a really powerful change. It helps senior leaders see why risk matters and supports better decisions.

Appendix One

Our audit approach

Our scope

1 We assessed how effectively government bodies manage risks to support better decisions and improve public service delivery. We examined leadership, governance, culture, capability and decision-making arrangements across government and assessed evidence against expectations for good practice in risk management, including the Orange Book, guidance developed by the Risk Centre of Excellence (CoE) and our previous work on managing risk in government. We reached our conclusions following analysis of documentary evidence, case studies, interviews, survey responses and other evidence collected mainly between March and July 2026.

2 We examined risk management in central government departments and arm's-length bodies (ALBs). We did not examine risk management in the devolved administrations, local government or government-owned companies. We also did not assess cross-government risk management arrangements such as the National Security Risk Assessment, which we have covered in previous work. While we considered the Risk CoE's role in setting expectations and supporting risk management across government, we did not assess its performance.

Our evidence base

Document review

3 We reviewed central government guidance, frameworks and supporting materials relating to risk management, governance, assurance and decision-making, including the *Orange Book*, *Teal Book* and guidance produced by the Risk CoE, such as the *Good Practice Guide: Risk Reporting*. We used these materials to identify good practice expectations against which we assessed government bodies. We also reviewed National Audit Office (NAO) and Public Accounts Committee reports, Government Internal Audit Agency's cross-government insight reports, other published material, and documentation from government departments and ALBs to inform our assessment of risk management in government.[17]

17 The Government Internal Audit Agency's insight reports are available to public sector officials on OneFinance (https://gff.civilservice.gov.uk/onefinance/) and KnowledgeHub (https://khub.net/group/guest/home).

Case studies and case examples

4 To understand how risk management operates in practice, we examined four government bodies as case studies: the then Department for Science, Innovation & Technology, the Ministry of Justice, the Rural Payments Agency and the UK Health Security Agency.[18] We selected these organisations to provide insight into how risk management is applied in different contexts and across a range of risk types, including operational, policy, delivery and strategic risks. In selecting case studies, we also sought diversity in organisational characteristics, such as size, functions and responsibilities. The case studies provided qualitative evidence on risk management arrangements and practices and are not statistically representative of the government as a whole.

5 For each organisation, we conducted at least three interviews with risk professionals, senior leaders (at the director and deputy director grade) and other stakeholders. We also reviewed a common set of documents, including risk management frameworks, risk registers, risk appetite statements and committee papers. We used this evidence to examine:

- governance, leadership and accountability arrangements for risk management;
- risk culture, skills and organisational capacity; and
- how risk management informs decision-making.

We analysed case study evidence against our audit questions.

6 In addition to case studies, we interviewed several government bodies to identify examples of good and improving practice ('case examples'). We selected examples through the survey, focus groups and conversations with the NAO's risk management experts and government officials. As with the case studies, we selected case examples to provide qualitative evidence and they are not statistically representative. We carried out semi-structured interviews with the then Department for Business & Trade, Department for Education, Government Property Agency, HM Land Registry, HM Revenue & Customs, Home Office, Ministry of Defence, National Highways, Network Rail, NHS Blood and Transplant and UK Hydrographic Office.

18 The Department for Science, Innovation & Technology was dissolved in July 2026 as part of a machinery of government change. Functions of the then department now sit within an expanded Department for Business, Innovation, Science & Trade, the Department for Digital, Culture, Media & Sport, and the Cabinet Office.

Interviews

7 In addition to the case study and case example interviews described above, we held regular discussions with officials from the Risk CoE to explore our audit questions and emerging findings. We also carried out semi-structured interviews with the Government Internal Audit Agency; the National Infrastructure and Service Transformation Authority; and Audit and Risk Assurance Committee Chairs at the four case study organisations, HM Prison & Probation Service, HM Courts & Tribunals Service and Active Travel England. We additionally engaged with the government's Heads of Risk Network and the Cross-Government Assurance Network to gather perspectives on risk management practices, challenges and emerging issues within individual organisations and across government.

8 The quotes from focus group participants and interviewees presented in this report have been edited for clarity and conciseness while remaining faithful to the speakers' meaning. They illustrate themes identified through our fieldwork and are not intended to represent the views of any individual organisation or the risk profession as a whole.

Survey

9 We conducted a cross-government survey of risk professionals working in government departments and ALBs. The survey covered leadership, culture, accountability, capacity, capability, risk-informed decision-making, and the influence of risk professionals. We used the survey results to identify common themes and differences between organisations. The results informed the content of focus groups (see below).

10 We developed the survey with input from the Risk CoE and internal quality assurance from the National Audit Office's Financial and Risk Management Insights team. The survey was hosted on a secure online platform. All questions were mandatory. Through the Risk CoE, we sought responses from organisations within the scope of the study and aimed to obtain at least one response from a wide range of departments and ALBs.

11 The survey was open for responses between 28 April and 8 June 2026. We received 68 responses from 39 organisations, including all 17 main government departments. Of these, 62 responses were within the scope of our study because respondents worked in a non-devolved department or ALB and were either senior civil servants with responsibility for risk management, or risk leaders and practitioners. We excluded six responses because the respondents' organisation or role was outside the scope of the study. Unless otherwise stated, findings in this report are based on the 62 in-scope responses. In a small number of cases, we made minor adjustments to rounded percentages when presenting survey results to ensure totals sum to 100%.

12 The survey generated quantitative and qualitative evidence, including free-text responses that provided additional examples. It was intended to capture the experiences and views of risk professionals across government, rather than to be statistically representative of all government bodies. As with many surveys, it is possible that there is a degree of selection bias in terms of our respondents. Because some respondents provided data anonymously, we cannot fully assess the extent of any selection bias. However, we found no indication that responses were skewed towards organisations with particular levels of risk management maturity.

Data analysis

13 We analysed responses to the annual Civil Service People Survey between 2017 and 2025 to gain insight into civil servants' views on risk culture across government. Specifically, we examined the percentage of respondents who answered 'agree' or 'strongly agree' to the statement: "In [my organisation], people are encouraged to speak up when they identify a serious policy or delivery risk." For each year, we calculated the median score across participating organisations and assessed variation between organisations using the range covering the middle 90% of scores, excluding the highest and lowest 5% of organisations. We used the full set of organisations included in the Civil Service People Survey dataset for each year. We excluded aggregate results where constituent organisations were also reported separately, to avoid double counting. We performed calculations using the published Civil Service People Survey data, which are rounded to whole percentages. As a result, the median scores presented in Figure 5 may differ slightly from the scores included in the Civil Service People Survey dataset due to rounding.

14 Unless otherwise stated, quantification of departmental Chief Risk Officers, principal risks and risk management software (paragraphs 13 and 2.13, 17 and 3.7, and 1.8, respectively) refers to the main government departments as at June 2026, prior to subsequent machinery of government changes. This analysis includes HM Revenue & Customs but excludes the Attorney General's Office, Northern Ireland Office, Office of the Advocate General for Scotland, Office of the Leader of the House of Commons, Office of the Leader of the House of Lords, Scotland Office, UK Export Finance and Wales Office.

Focus groups

15 We conducted online focus groups with government risk professionals in May and June 2026. We held four focus groups, with 21 participants representing 17 government departments and ALBs. We used focus groups to explore the results of our cross-government survey, test findings, gather illustrative quotes and gain insight into challenges and good practice. The focus groups were not designed to provide statistically representative evidence.

16 The focus groups followed a semi-structured approach, with a set of core questions supplemented by guided discussion and follow-up questions. Core questions covered:

- risk teams' capacity and skills;
- risk professionals' ability to influence decision-making;
- the role of senior leaders in supporting change;
- risk culture; and
- risk appetite.

We analysed focus groups transcripts thematically.

International insights

17 We undertook a light-touch review of international practice to provide context for our findings and identify examples of relevant practice and innovation. We did not assess the relative performance of different countries. Differences in institutional arrangements mean that practices are not always comparable.

18 We reviewed relevant publications from overseas supreme audit institutions, governments and international organisations. We submitted an information request to the supreme audit institutions of Australia, Canada, Ireland, the Netherlands, Singapore, South Korea, Sweden, Switzerland and the United States. Our information request covered risk management responsibilities and skills, examples of effective and ineffective risk management, and relevant audit work. We selected these countries through desk-based research and discussions with NAO risk experts.

19 We additionally held semi-structured interviews with officials of the European Court of Audit, Audit Wales, the Scottish Government and the City of Edinburgh Council.

Engagement with experts

20 As part of our quality assurance and internal consultation procedures, we engaged expert members of the NAO's Financial and Risk Management Insights team, People and Operational Management Insights team, and the organisation's internal risk and governance team.

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: 018285-001

£10.00
ISBN: 978-1-78604-702-1