NAO
National Audit Office

REPORT

Government cyber resilience

Cabinet Office

SESSION 2024-25
29 JANUARY 2025
HC 546

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 2023, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £1.59 billion. This represents around £17 for every pound of our net expenditure.

Government cyber resilience

Cabinet Office

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 27 January 2025

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

21 January 2025

HC 546 | £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.

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.

014935 01/25 NAO

Contents

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:

Alice Broughton,
Elizabeth Hogarth, Daniel Kintoff and Jonathan Pownall, under the direction of Tom McDonald and Yvonne Gallagher.

For further information about the National Audit Office please contact:

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

☎ 020 7798 7400

www.nao.org.uk

@NAOorguk

Key facts

Multiple

system controls fundamental to departments' cyber resilience were at low levels of maturity in 2024, including asset management, protective monitoring and response planning

At least 228

'legacy' IT systems in use by departments in March 2024, and the government does not know how vulnerable these are to cyber attack

More than 50%

of roles in several departments' cyber security teams were vacant in 2023-24

89	of the 430 incidents managed by the National Cyber Security Centre between September 2023 and August 2024 were assessed as "nationally significant"
£600,000	the British Library's assessment of the financial costs that could be directly attributed to the October 2023 cyber attack it experienced, by March 2024
32%	of roles in the Government Security Group's (GSG) cyber directorate were vacant when GSG established it in November 2022
£1.3 billion	additional funding provided to departments and intended for investment in cyber and 'legacy' IT over the 2021 Spending Review period

Summary

Introduction

1 Cyber attack is one of the most serious risks to the UK and the government's resilience. The COVID-19 pandemic highlighted that the UK needed to strengthen its national resilience and prepare for future emergencies. The government defines cyber resilience as "the ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events".

2 The need for the government to improve its cyber resilience is becoming more urgent in an increasingly digital world. The last decade has seen rapid growth in the government's digital ambitions, the number of government services available online, and the devices and IT systems that connect people, organisations and businesses globally. This provides significant opportunities for society and the economy. It also makes it easier for those with malicious intent to cause disruption, which can have a devastating impact on individuals, government organisations and public services. The cyber threat to the UK comes from a range of 'threat actors' (individuals, groups or organisations that intentionally cause harm to digital devices or systems). Threat actors include those who are 'state-affiliated' and funded by states and governments; those who are 'state-aligned', who are often not subject to state control and are ideologically rather than financially motivated; and financially motivated cyber criminals or groups.

3 The UK's cyber security and resilience has been a strategic priority for government for at least a decade. In 2010, the National Security Strategy described cyber attack as a top threat and priority for action. The government supported its 2011 UK Cyber Security Strategy with a £650 million cross-government National Cyber Security programme. It supported the subsequent National Cyber Security Strategy 2016–2021 with funding of £1.9 billion. We examined both strategies and programmes in previous reports. We found that the government had made some good progress with its 2016 programme, such as by creating the National Cyber Security Centre (NCSC), the UK's technical authority on cyber security, but that it was unclear whether the government would achieve its strategic objectives.

4 In January 2022, the Cabinet Office published the Government Cyber Security Strategy: 2022–2030 ('the Strategy') which, for the first time, set out the challenges facing government cyber security and a vision for improving it. The Strategy aligns with the 2021 Integrated Review of Security, Defence, Development and Foreign Policy and the National Cyber Strategy 2022 in supporting the government's ambition to make the UK a democratic and responsible cyber power. The vision of the Strategy is to "ensure that core government functions, from the delivery of public services to the operation of national security apparatus, are resilient to cyber attack".

5 In the July 2024 King's Speech, the government announced it would introduce a Cyber Security and Resilience Bill. The aim of the Bill is to strengthen the UK's cyber defences to ensure that the critical infrastructure and digital services companies rely on are secure.

6 The Government Security Group (GSG) in the Cabinet Office leads the government's security function, including cyber security. It is responsible for leading implementation of the Strategy and supporting government departments to improve their cyber resilience. GSG works closely with the NCSC and the Central Digital and Data Office (CDDO), which leads the government's digital and data function. Departments are responsible for their own cyber resilience and meeting the security standards set by GSG. They also are responsible for ensuring their sectors and arm's-length bodies meet strategic resilience targets.

7 In December 2022, government published the *UK Government Resilience Framework*, setting out its strategic approach to strengthening resilience. Our report is part of our programme of work on resilience and follows our previous reports on *Government resilience: extreme weather* and *Resilience to flooding.*[1]

Scope of this report

8 This report examines whether the government's efforts to improve its cyber resilience are keeping pace with the cyber threat it faces. The report aims to: hold government to account for its performance; increase transparency about how cyber resilient government is; and help government improve its cyber resilience. To do this, we examined:

- the threat to government cyber security;
- progress with implementing the Strategy;
- the government's cyber resilience position in 2024; and
- the challenges for departments in building cyber resilience.

[1] Comptroller and Auditor General, *Government resilience: extreme weather*, Session 2023-24, HC 314, National Audit Office, December 2023; and Comptroller and Auditor General, *Resilience to flooding*, Session 2023-24, HC 189, National Audit Office, November 2023.

9 We have undertaken this report at this time because the government has assessed that the cyber threat is rapidly increasing, has started collecting detailed and reliable data on its cyber resilience in 2024, and planned to achieve key parts of the Strategy by 2025. This report focuses on the cyber resilience of ministerial and non-ministerial departments and their arm's-length bodies (which we refer to in this report as 'departments'). This report does not cover the cyber resilience of local government, public corporations, businesses or UK society more widely. This report focuses on the cyber resilience of IT systems at the 'official' level of security classification and not systems classified as 'secret' or above.

Evaluative criteria

10 To assess if the government's efforts to improve its cyber security are providing value for money, we considered whether:

- the centre of government has set clear, risk-based cyber resilience outcomes for departments to meet; or
- provided the right support and incentives to allow departments to do so; and whether
- departments have appropriately prioritised, and built the capability to deliver, the cyber security they need to operate effectively.

Key findings

The threat to government cyber security

11 The size, diversity and age of the government's digital estate makes it challenging for government to be cyber resilient. Departments, arm's-length bodies and their partners use a wide range of IT systems and technology to provide public services. The breadth and diversity of these systems make it difficult for the government to assess overall cyber resilience. Many of these systems can be described as 'legacy', because they are ageing and outdated but still in use. Legacy systems are often more vulnerable to cyber attack because their creators no longer update or support their use, few people have the skills to maintain them, and they have known vulnerabilities. The government estimated that it used nearly half of its £4.7 billion IT expenditure in 2019 to keep legacy systems running. Risks to public services posed by legacy technology have built up over many years (paragraphs 1.2 to 1.3).

12 **The threat the government faces from cyber attack is rapidly evolving and is the most sophisticated it has ever been.** In December 2024, the NCSC warned of a “diffuse and dangerous” cyber threat to UK society, which grows more complex every year. Highly capable state and state-aligned actors, including from China, Russia and Iran, are using increasingly sophisticated methods to carry out malicious cyber activity. Cyber threat actors can easily access commercially and publicly available tools and services, including those provided by criminals. This enables them to perform a variety of cyber attacks, which could affect the government and the wider public sector. In December 2024, the NCSC described a “widening gap between the increasingly complex threats and our collective defensive capabilities in the UK, particularly around our critical national infrastructure”. In December 2023, Parliament’s Joint Committee on the National Security Strategy warned there was a high risk of a catastrophic ransomware attack at any moment. Both the cyber threat and government’s cyber security capability continue to evolve as technology develops. For example, artificial intelligence can help to improve the government’s cyber security but it can also help threat actors looking to interfere or undermine trust in our democratic system (paragraphs 1.4 to 1.8).

13 **Cyber attacks have devastating effects on government organisations, public services and people’s lives**. Cyber threat actors routinely target government organisations. Between September 2020 and August 2021, around 40% (around 310) of the 777 incidents managed by the NCSC, because of their potential severity, were aimed at public sector organisations, including central and local government, emergency and health services, and law enforcement. The NCSC assessed that 89 of the 430 incidents it managed because of their potential severity, between September 2023 and August 2024, were “nationally significant”. Cyber attacks can affect every aspect of an organisation’s operation, and recovery is often lengthy and costly. For example, in October 2024, the British Library was still rebuilding its research services and IT systems a year after the cyber attack it experienced. Although the Library remained open following the attack, its research services were severely restricted in the first two months and remained incomplete following the return of a searchable version of its online catalogue in January 2024. The Library reported that the directly attributable additional costs resulting from the cyber attack totalled £600,000 by March 2024. Cyber attacks can have devastating consequences for individuals if they cannot access critical services or if their data are stolen. In June 2024, the cyber attack on a supplier of pathology services to the NHS in south-east London led to two NHS foundation trusts postponing 10,152 acute outpatient appointments and 1,710 elective procedures (paragraphs 1.9 to 1.11, Figure 1 and Appendix Two).

Progress with implementing the Government Cyber Security Strategy

14 **GSG's resource constraints have limited how quickly it could implement centrally led interventions and the extent it could support departments.** In November 2022, GSG created a cyber directorate to lead the government's cyber security function, support departments to implement the Strategy, and to lead interventions to improve government cyber resilience. The cyber directorate consistently reported resourcing, including recruitment and retention of staff, as a significant problem affecting the progress of its work. It had a significant shortage of staff, with around 32% of posts vacant, when it was first established. Given its resource constraints, the cyber directorate prioritised the interventions it could lead from the centre of government. Between 2022 and 2024, its work included developing 'GovAssure' (a cyber security assurance scheme) to build organisational resilience and creating a Government Cyber Coordination Centre (GC3) to help government "defend as one". The cyber directorate made limited progress in leading work to meet other strategic objectives that would help to improve government cyber resilience, such as helping departments to develop the right cyber security skills, knowledge and culture (paragraphs 2.2 to 2.5 and Figure 2).

15 **Until April 2023, the government did not collect detailed, reliable data about the cyber resilience of departments.** Before 2023, GSG asked departments to self-assess their performance against the minimum cyber security measures it had set for them. This did not give the government a good understanding of the cyber resilience of departments or specific IT systems. GSG used these limited and subjective data to estimate that 25% of government organisations were meeting the minimum standards in 2022. In April 2023, GSG started using the NCSC's cyber assessment framework (CAF) to agree with departments what cyber resilience outcomes they needed to achieve based on their role, likelihood of being targeted by a threat actor, IT estate, and the level of risk they were prepared to take. GSG asked departments to use GovAssure to assess their cyber resilience and get independent reviewers to verify their performance. Between April 2023 and July 2024, GSG used GovAssure to begin collecting detailed, reliable data about how cyber resilient some of departments' most important IT systems were. This has provided better information than its previous approach of relying on departments' self-reported cyber resilience (paragraphs 2.6 to 2.9 and Figure 3).

16 **The government has not improved its cyber resilience quickly enough to meet its aim to be "significantly hardened" to cyber attack by 2025.** The GovAssure process involves GSG agreeing targeted improvement plans (TIPs) with departments to remediate the priority issues identified. By August 2024, GSG had agreed TIPs with departments. By November 2024, GSG had not commissioned progress updates but planned to do so once departments had had more opportunity to implement their TIPs. Departments will not be able to confirm whether TIPs are fully funded until the 2025 Spending Review concludes. CDDO has created an approach known as 'Secure by Design', which aims to build effective cyber security practices into new digital services and technical infrastructure. This approach could help departments in the long term, but CDDO does not expect that it will start improving services across the whole public sector until 2026. It is therefore unlikely to significantly contribute towards the Strategy's aims for the government to be "significantly hardened" to cyber attack by 2025, and the whole public sector to be resilient to known attacks by 2030 (paragraphs 2.10 to 2.14).

17 **Although the government has improved its coordination of cyber security, departments still find it difficult to understand the roles and responsibilities of the cyber organisations at the centre of government.** In 2016, we reported that the government's failure to coordinate how it protects information meant that many organisations had overlapping mandates and activities. In October 2016, the government successfully consolidated four organisations into the NCSC. In 2023, the Cabinet Office created the GC3. The GC3 is a collaborative partnership between GSG, CDDO and the NCSC to coordinate cyber security efforts across government so that it can "defend as one". Nonetheless, some departments did not understand the extent to which GSG or the NCSC are responsible for government's cyber resilience and incident management. There are opportunities for GSG to improve how the centre of government communicates with departments, for example, in providing advice on the cyber threat and how to respond to it. There are still challenges for GSG and CDDO to overcome in how they coordinate to build cyber security into government's digital strategies and services following the government's decision to move CDDO from the Cabinet Office to the Department for Science, Innovation & Technology (paragraphs 2.15 to 2.19 and Figure 4).

18 GSG has not had sufficient measures in place to show whether its work to strengthen government's cyber security is effective, nor does it have a plan for how government organisations could become cyber resilient by 2030. By January 2025, GSG had not created a comprehensive monitoring and evaluation framework or shared a cross-government strategy implementation plan with departments. This means GSG has not yet been able to effectively measure, monitor and evaluate the government's progress towards the Strategy's aims for 2025 and 2030, or show how well its initiatives are working, and why. Without a cross-government implementation plan, various parts of government, including departments, do not know what they need to do and by when. GSG's shortage of staff meant it has not put in place robust arrangements to oversee how departments are implementing the Strategy. For instance, in April 2024, GSG asked departments to start developing their own implementation plans, but since then it has not asked for regular progress reports. GSG is learning from the experience of international partners on how to provide more centralised capability and support to departments (paragraphs 2.20 to 2.23).

Government's cyber resilience position in 2024

19 The first year of GovAssure identified significant gaps in departments' cyber resilience, which means they are vulnerable to cyber attack. Between April 2023 and July 2024, 35 departments took part in the first year of GovAssure and self-assessed 72 IT systems, which they identified as critical to running their most important services. Independent reviewers assessed 58 of these. GovAssure data found significant gaps in departments' cyber resilience. The data highlighted multiple fundamental system controls that were at low levels of maturity across departments including asset management, protective monitoring, and response planning. GSG reported to ministers the implication of these findings: the cyber resilience risk to government was extremely high (paragraphs 3.2 to 3.4).

20 The government does not have a detailed understanding of the resilience of its legacy IT systems. In September 2023, CDDO published its legacy IT risk assessment framework. It used this to collect departments' assessments of the risks associated with their legacy systems and information on departments' plans to remediate them. These risk assessments were not detailed and included aspects of cyber security in addition to other criteria. In March 2024, departments reported using at least 228 legacy IT systems. Of these, 28% (63 of 228) were red-rated as there was a high likelihood and impact of operational and security risks occurring. GSG did not include legacy systems in GovAssure because many of its recommended system controls would not be applicable to legacy systems. This means GSG and CDDO do not have a detailed assessment of:

- the cyber security risk to departments and their essential services caused by using legacy IT; or
- how well departments have managed this risk, for example, by isolating legacy IT from the rest of their network or performing vulnerability assessments (paragraphs 3.5 to 3.7).

Challenges for departments in building cyber resilience

21 **Departments have not met their responsibilities to improve their own and their wider sectors' cyber resilience.** Leaders within departments have not always recognised how cyber risk is relevant to their strategic goals. Often, departments' most senior decision-making boards and non-executive boards do not include any digital leaders or directors with cyber expertise. In April 2024, GSG recommended to ministers that departments strengthen their accountability for cyber risk through improved reporting and risk management. In 2024, GovAssure data showed that departments were not meeting their responsibility to be cyber resilient. Additionally, the government did not have sufficient oversight of the cyber resilience of the wider public sector, which lead government departments are responsible for. In April 2024, GSG reported that departments cited insufficient funding, number of staff, and oversight mechanisms as barriers to understanding and improving cyber resilience across the bodies they oversee. Some departments have been reluctant to share information about their cyber incidents with other parts of government, which has limited the opportunities for other organisations to learn and improve their own cyber resilience (paragraphs 4.2 to 4.9).

22 **Departments' funding of other priorities and management of their financial pressures has reduced the scope of departments' cyber security work, which could increase the severity of a cyber attack when it happens.** Departments' accounting officers are responsible for making decisions that protect the security of their organisations. In the 2021 Spending Review, the government announced it would invest £2.6 billion in cyber, of which it allocated £1.3 billion to departments for cyber security and legacy IT remediation. By January 2023, departments had funded the most urgent cyber priorities but risked not meeting their cyber resilience targets due to financial pressures. Since January 2023, some departments have significantly reduced the scope of their cyber security improvement programmes to fund other priorities. In March 2024, departments did not have fully funded plans to remediate around half of the government's legacy IT assets (53%, or 120 out of 228), leaving these systems increasingly vulnerable to cyber attack. Under-investment in technology and cyber security played a role in the severity of the cyber attack on the British Library (paragraphs 4.10 to 4.14 and Figures 5 and 6).

23 **The government finds it difficult to recruit and retain enough people with cyber skills and to upskill its existing workforce.** For more than a decade, skilled cyber security professionals have been in short supply and high demand nationally and globally. In 2023-24:

- one in three cyber security roles in central government was either vacant or filled by temporary staff (contingent labour);
- the proportion of vacancies in several departments' cyber security teams was more than 50%; and
- 70% of specialist security architects in post were temporary staff.

Departments reported that the salaries they can pay and civil service recruitment processes are barriers to hiring and keeping people with cyber skills. The Cabinet Office's cyber skills initiatives overlap with departments' own cyber skills programmes, which departments cannot always use because of government restrictions on the number of people employed. In January 2025, GSG's strategy to reduce the gap between the cyber skills the government has and the cyber skills it needs by 2030 was partially funded. The persistence of cyber skills shortages shows that the government may need to take a different approach to get the right cyber skills in government (paragraphs 4.15 to 4.19 and Appendix Three).

Conclusion

24 Cyber attacks continue to have serious consequences for government organisations, public services and people's lives, undermining the value for money of government expenditure in affected services and systems. The cyber threat to the government is severe and advancing quickly. In response, the Cabinet Office has published and started leading work to implement the first cyber strategy for government. Its work on centrally led interventions such as GovAssure and Secure by Design should improve departments' cyber resilience.

25 However, progress is slow and cyber incidents with a significant impact on government and public services are likely to happen regularly, not least because of the growing cyber threat. The government's cyber resilience levels are lower than it previously estimated, and departments have significant gaps in their system controls that are fundamental to their cyber resilience. The resilience of the hundreds of ageing legacy IT systems that departments still use is likely to be worse, and departments have no fully funded remediation plans for half of these vulnerable systems. As a result, the government will not meet its aim for its "critical functions" to be resilient to cyber attack by 2025. GSG assesses that achieving this for the wider public sector by 2030 remains ambitious, in part because this relies on departments meeting their responsibilities to keep their systems cyber resilient.

26 To avoid serious incidents, build resilience and protect the value for money of its operations, government must catch up with the acute cyber threat it faces. The government will continue to find it difficult to do so until it successfully addresses the long-standing shortage of cyber skills, strengthens accountability for cyber risk, and better manages the risks posed by legacy IT.

Recommendations

The centre of government

a **Within six months, GSG should develop, share and start using a cross-government implementation plan for the Government Cyber Security Strategy: 2022–2030 (‘the Strategy’).** GSG should refresh it regularly, include how the government is responding to new and severe cyber threats not covered by the Strategy and:

- bring together a comprehensive monitoring and evaluation framework that allows GSG to measure departments’ performance, track and show progress towards the Strategy’s outcomes, and evaluate what is working well or not, including an assessment of lessons learned from previous efforts to attract, upskill and retain cyber skills in government; and
- identify the priority actions the government needs to take to be cyber resilient by 2030, the government organisations that are accountable for those actions, the timescales within which those actions need to be taken, and the extent to which those organisations have the resource and levers needed to complete their actions.

b **Within six months, GSG should set out how the whole of government needs to operate differently, and what is needed for this transformation to be effective, so that the government can achieve its goals for cyber security and resilience.** GSG should work with the relevant bodies at the centre of government to develop and agree what governance, type and amount of funding, people and skills, and organisational structure and mandate will best enable government to achieve its objectives. This should include setting out how the centre of government will:

- provide different types of support, capability and guidance to departments;
- build cyber security into its digital and technology strategies, plans and activity from the outset; and
- clarify which aspects of cyber risk and resilience departments, GSG and other organisations are responsible for and when that responsibility moves from one organisation to another.

c **GSG should strengthen GovAssure's focus on improving cyber resilience outcomes.** GSG should:

- continue building the capacity to support departments in developing and implementing targeted improvement plans, and monitoring and evaluating progress against them;
- continue developing how GovAssure data can be used to measure departments' performance as part of its comprehensive monitoring and evaluation framework; and
- baseline government organisations' cyber resilience against organisations that are responsible for UK critical national infrastructure.

d **GSG should work with CDDO to take a more rigorous approach to understanding and mitigating the risk to government organisations' cyber resilience caused by legacy IT systems.** Learning from GovAssure and the legacy IT risk assessment framework, this approach should:

- identify the legacy systems in use across government;
- understand the risk these legacy IT systems pose to cyber resilience, the extent of departments' remediation plans, and be risk-based when prioritising security enhancements;
- assess and strengthen the security enhancements that are in place; and
- be considered alongside GovAssure when measuring government organisations' cyber resilience and performance.

e **GSG should design regular communications to ensure that senior leaders and other decision-makers across government understand the cyber threat, how it is relevant to their business outcomes and what they can do about it.** GSG should embed this into departments' board and programme governance.

Departments

f **Government departments should urgently strengthen their own governance, accountability and reporting arrangements around cyber risk.** In their annual security appraisal, accounting officers should assess their progress and performance in meeting the cyber security standards set out in Functional Standard GovS 007: Security (the Security Standard), which HM Treasury mandated in 2021. To show the importance of building a cyber security culture, accounting officers should:

- ensure that membership of their most senior decision-making board includes at least one digital leader with cyber expertise and one non-executive director with cyber expertise;
- engage with GSG to agree how the department will contribute to GSG's cross-government implementation plan;
- understand the cyber risk posed by their most critical IT systems and create and test appropriate incident response plans; and
- commission reporting that shows progress made in implementing the Strategy.

g **Working in alignment with GSG's government skills strategy, departments should make and enact plans to fill the cyber skills gaps in their workforces.** Within the next year, they should:

- undertake a gap analysis of their current cyber workforce to identify what skills are needed to enable effective implementation of the Strategy; and
- present clear and detailed improvement plans to GSG.

Part One

The threat to government cyber security

1.1 It is important that the UK can protect and promote its interests in a world shaped by technology. Cyber attacks increasingly threaten the government's ability to safeguard national security and run public services. This part sets out:

- the challenge of cyber security for the government's digital estate;
- the cyber threat; and
- the effect cyber attacks have on government organisations, public services and people's lives.

The challenge of cyber security for the government's digital estate

1.2 The size, diversity and age of the government's digital estate makes it challenging for government to be cyber resilient. Government departments and arm's-length bodies provide government functions and services, often through contracts with private and voluntary providers. These providers use a wide range of IT systems and technology that can potentially act as an entry point for a threat actor, or become a source of instability if they suffer an incident. This makes it difficult for the government to know how many IT systems exist, or to assess their cyber resilience.

1.3 Ageing and outdated IT systems (hardware and software), known as 'legacy', increase the government's exposure to cyber attack. The reasons for this include: their creators no longer update or support their use; few people have the skills to maintain them; they are often incompatible with modern security and access control features; and they have known vulnerabilities. Legacy IT systems can be used as an entry point for threat actors to access and move across a network. The government estimated that it used nearly half of its £4.7 billion IT expenditure in 2019 to keep legacy systems running. Risks to public services posed by legacy technology have built up over many years. We have previously reported that government departments:

- typically do not have a good understanding of their IT estate and its interdependencies;
- often poorly understand legacy systems because of their age; and
- have historically under-invested in these systems.

The cyber threat

1.4 The cyber threat to government is rapidly evolving. Cyber threat actors (individuals or groups posing a threat to cyber security) continue to pursue government data for strategic advantage or seek to disrupt public services for financial or political gain. The government expects that, as it strengthens its cyber defences, threat actors will also change and improve in response.

State-affiliated cyber threat actors

1.5 In October 2024, the Head of MI5 described how "autocratic regimes" invest heavily in advanced cyber operations. He said: "Their targets include sensitive government information, our technology, our democracy, journalists and defenders of human rights." In December 2024, the National Cyber Security Centre (NCSC) warned of a "diffuse and dangerous" threat from states and state-aligned groups to the everyday functioning of society in the UK, which grows more complex every year. The NCSC highlighted that:

- China was a highly sophisticated and capable threat actor with an intent to threaten essential sectors such as energy, transportation and water;
- Russia continued to be a "capable, motivated and irresponsible" actor in cyberspace and had inspired non-state threat actors to attack critical national infrastructure; and
- Iran remained aggressive in cyberspace and continued to achieve its objectives through less sophisticated cyber techniques.

1.6 The cyber threat to government from state-affiliated actors is the most sophisticated it has ever been. In December 2024, the NCSC described a "widening gap between the increasingly complex threats and our collective defensive capabilities in the UK, particularly around our critical national infrastructure". The NCSC has warned that state-affiliated actors are trying to covertly access important networks and systems with the intention of making use of that access at a later date, and this could allow them to disrupt critical national infrastructure at a time of their choosing. In February 2024, the NCSC published details of how threat actors were using advanced cyber techniques to gain persistent access to victims' IT systems and avoid detection. In May 2023, Microsoft reported that attackers had used a cyber attack technique, known as 'living off the land', to compromise US critical national infrastructure.

Ransomware and extortion attacks

1.7 Ransomware and, increasingly, data theft and extortion, are acute cyber threats to the UK. Threat actors can easily access commercially and publicly available tools and services, including those provided by criminals. This enables them to perform a variety of cyber attacks, which could affect the government and the wider public sector. Stealing and encrypting data is the primary tactic cyber criminals use to make money. Ransomware is malware that prevents a victim from accessing their device and the data stored on it, usually by encrypting the stolen files. The threat actor will demand a ransom in exchange for decryption. Threat actors may also threaten to leak the data they steal. Some groups conduct data theft and extortion by saying they will stop a cyber attack if victims pay them money. In December 2023, Parliament's Joint Committee on the National Security Strategy warned that the UK's legislative framework was outdated and the government's failure to invest sufficiently meant there was a high risk of a catastrophic ransomware attack at any moment.[2]

New technologies

1.8 The cyber threat continues to evolve as technology develops, but this also gives government opportunities to improve its cyber security capability. For example, artificial intelligence (AI) can improve government's cyber security, but it can also help threat actors looking to interfere or undermine trust in our democratic system. The NCSC is collaborating with its partners to realise the benefits of AI and protect against the associated security risks. Other technologies the NCSC considers important include semiconductors (as core components of all electronic devices), post-quantum cryptography (that will keep data safe from future large-scale quantum computers), telecoms security, and assessing risks from radio frequency transmissions. There is a risk that threat actors take advantage of new technologies faster than the government.

The effect of cyber attacks on organisations and people

1.9 The NCSC and the National Crime Agency have set out how cyber attacks can affect every aspect of an organisation's operation. This can include damaging finances, compromising customer data, disrupting operational delivery, eroding trust and damaging reputations. Threat actors targeting essential services such as healthcare can pose a real risk to public safety and have devastating consequences for individuals.[3] For example, cyber attacks can mean that individuals can no longer access critical services, or may have their personal data stolen. In June 2024, the cyber attack on a supplier of pathology services to the NHS in south-east London led to King's College Hospital NHS Foundation Trust, and Guy's and St Thomas' NHS Foundation Trust postponing 10,152 acute outpatient appointments and 1,710 elective procedures.

[2] Joint Committee on the National Security Strategy, *A hostage to fortune: ransomware and UK national security*, First Report of Session 2023-24, HC 194, December 2023.

[3] National Cyber Security Centre and National Crime Agency, *Ransomware, extortion and the cyber crime ecosystem*, September 2023.

1.10 Organisations that are the victims of cyber attack may feel short- and long-term impacts, particularly if they were unprepared. Recovery is often lengthy and costly. For example, the impact of the cyber attack on the British Library that took place in October 2023 was extensive and, by January 2025, not fully resolved. Although the Library remained open throughout, its research services were severely restricted in the first two months and remained incomplete following the return of a searchable version of its online catalogue in January 2024. The directly attributable additional costs resulting from the cyber attack totalled £600,000 by March 2024.[4] In October 2024, a year after the attack, the Library was still rebuilding its systems.

1.11 The Government Cyber Security Strategy: 2022–2030 ('the Strategy') reported that government organisations are "routinely and relentlessly targeted" by threat actors. The NCSC assessed that 89 of the 430 incidents it managed because of their potential severity between September 2023 and August 2024, were "nationally significant". This included cyber attacks in a range of sectors. There is no single source of data that shows the prevalence of the cyber threat to the public sector or to government IT systems. **Figure 1** shows indicators of the scale and severity of the cyber threat to the UK and central government using the available data. Appendix Two shows examples of how cyber attacks have affected government departments and public bodies in recent years, including the Ministry of Defence, the Electoral Commission and Parliament.

[4] British Library, *Annual Report and Accounts 2023 to 2024*, July 2024.

Figure 1

Indicators of the scale and severity of the cyber threat to the UK and central government

Most indicators show that the cyber threat has increased in scale[1]

Measure	Scale	Trend	Severity
Number of cyber attacks reported to the National Cyber Security Centre (NCSC).	1,957 cyber attacks were reported to the NCSC between September 2023 and August 2024.	3% decrease, down from 2,005 reported between September 2022 and August 2023.	The NCSC managed 430 cyber attacks reported to it, of which 89 were "nationally significant".
Proportion of cyber incidents managed by the NCSC that targeted the public sector.[2]	Around 40% (around 310) of the 777 incidents managed by the NCSC between September 2020 and August 2021 targeted the public sector.	–	The NCSC manages those cyber incidents it categorises as having significant severity and impact.
Cyber incidents reported to the Information Commissioner's Office (ICO) by central government.	Up to 114 breaches reported to the ICO between July 2023 and June 2024.[3]	75% increase, up from 65 reported between July 2022 and June 2023.	Data of more than 100,000 people affected.
Cyber Security Breaches Survey 2024: an annual official statistic detailing the cost and impact of cyber security breaches and attacks on businesses, charities and educational institutions.	Around 50% of UK businesses (718,000) experienced some form of cyber security breach or attack in the 12 months before they responded to the winter 2023-24 survey.	– [4]	Around 13% of the businesses affected experienced financial or data loss and 24% experienced other negative impacts, such as disruption to staff.
Crime Survey for England and Wales (CSEW) estimates for computer misuse incidents.	In 2023-24, there were an estimated 1,022,000 incidents of computer misuse, including use of viruses and hacking.	37% increase, up from an estimated 745,000 incidents in 2022-23.	–
Microsoft reporting on the countries that state-affiliated threat actors target most.	In 2024, the UK was the second most targeted country in Europe and the fifth most targeted country in the world.	In 2023, the UK was the second most targeted country in Europe.[5]	–

Notes

1 There are no publicly available data that show the number and severity of cyber attacks experienced by central government. As such, the data presented provide an indication of the general prevalence of the cyber threat.

2 The National Cyber Security Centre (NCSC) defined the public sector as including local government, central government, the devolved administrations as well as political, intelligence, emergency and health services, and law enforcement. The NCSC chooses which incidents to manage based on its evaluation of their severity and potential impact on the UK.

3 Central government may have reported fewer breaches to the Information Commissioner's Office (ICO) than shown. This is because the ICO presents the breaches reported to it by the number of types of data affected.

4 In 2024, how the Cyber Security Breaches Survey asked about the overall incidence of cyber attacks was changed, preventing direct comparison with 2023.

5 In 2023, Microsoft did not report how often the UK was targeted compared with other countries on a global basis.

Source: National Audit Office analysis of publicly available reports and statistics

Part Two

Progress with implementing the Government Cyber Security Strategy

2.1 This part sets out the aims of the Government Cyber Security Strategy: 2022–2030 ('the Strategy') and assesses the progress the Government Security Group (GSG) has made in leading its implementation.

The Government Cyber Security Strategy: 2022–2030 ('the Strategy')

2.2 The Strategy was the first strategy that focused only on the government's cyber resilience, rather than the cyber security of the UK as a whole (**Figure 2**). In its definition of 'government', the Strategy included departments, arm's-length bodies, agencies and local authorities, recognising that many diverse public sector organisations deliver core government functions. The Strategy highlighted "a significant gap between where government cyber resilience is now and where it needs to be". The aim of the Strategy is for:

- "government's critical functions to be significantly hardened to cyber attack by 2025"; with
- "all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030".

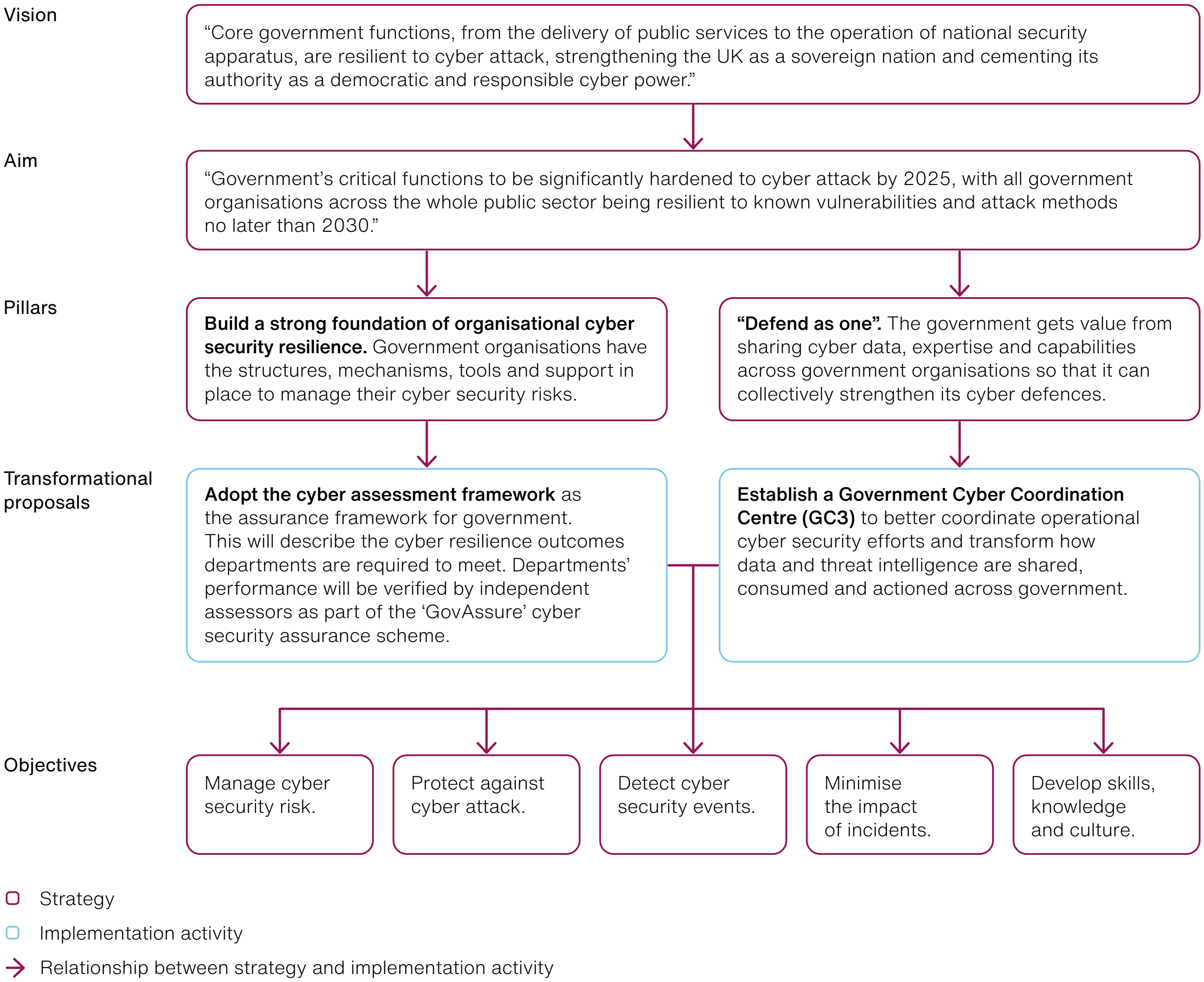
2.3 The Strategy has two strategic 'pillars' that define the government's approach to cyber resilience. These are:

- to build a strong foundation of organisational cyber security resilience; and
- for government organisations to "defend as one" by working together collaboratively so that the government can meet the scale of the challenges it faces.

Figure 2

The Government Cyber Security Strategy: 2022–2030 (‘the Strategy’)

In delivering the Strategy, the government has prioritised implementing two transformational proposals



Vision

“Core government functions, from the delivery of public services to the operation of national security apparatus, are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.”

Aim

“Government’s critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.”

Pillars

Build a strong foundation of organisational cyber security resilience. Government organisations have the structures, mechanisms, tools and support in place to manage their cyber security risks.

“Defend as one”. The government gets value from sharing cyber data, expertise and capabilities across government organisations so that it can collectively strengthen its cyber defences.

Transformational proposals

Adopt the cyber assessment framework as the assurance framework for government. This will describe the cyber resilience outcomes departments are required to meet. Departments’ performance will be verified by independent assessors as part of the ‘GovAssure’ cyber security assurance scheme.

Establish a Government Cyber Coordination Centre (GC3) to better coordinate operational cyber security efforts and transform how data and threat intelligence are shared, consumed and actioned across government.

Objectives

Manage cyber security risk.

Protect against cyber attack.

Detect cyber security events.

Minimise the impact of incidents.

Develop skills, knowledge and culture.

□ Strategy

□ Implementation activity

→ Relationship between strategy and implementation activity

Source: National Audit Office analysis of the Government Cyber Security Strategy: 2022–2030

GSG's performance in leading the implementation of the Strategy

2.4 In November 2022, GSG created a cyber directorate to lead the government's cyber security function and support departments to implement the Strategy. By July 2023, GSG considered that it had effectively established the cyber directorate, which was providing clear strategic direction. The cyber directorate has consistently reported resourcing, including recruitment and retention of staff, as a significant problem affecting its progress in implementing the Strategy. When GSG set up the cyber directorate, 32% of the roles it planned to recruit were vacant. Until mid-2023, GSG reported finding it difficult to recruit because of government-wide recruitment restrictions and lengthy Cabinet Office approval processes. By May 2024, this improved to around 12% of roles vacant.

2.5 Given its resource constraints, GSG prioritised a range of interventions it could make from the centre of government between 2022 and 2024. These included two implementation activities intended to transform government's cyber resilience (transformational proposals):

- Develop a cyber security assurance scheme (GovAssure) to verify departments' performance against the cyber assessment framework (CAF).
- Create the Government Cyber Coordination Centre (GC3).

GSG made limited progress on other important objectives of the Strategy, such as helping departments to develop the right cyber security skills, knowledge, and culture. This was because GSG lacked resources (both people and budget) to carry out this work alongside its existing work to develop cyber skills.

Strategic pillar one: Building organisational resilience

2.6 To build greater cyber resilience across departments, the government's plans included:

- the GovAssure cyber security assurance scheme; and
- introducing a 'Secure by Design' approach to new digital systems or changing existing ones.

Cyber assessment framework and GovAssure

2.7 The government has been slow to gather detailed and reliable data on its cyber security and resilience. GSG oversees government security and sets standards of security that government organisations must meet. In 2018, GSG introduced minimum cyber security standards (MCSS) that set out the minimum cyber security measures it expected departments to meet. GSG checked compliance with these, and its other security standards, through a 'departmental security health check'. Departments completed the annual security health check by self-assessing their performance, which was not validated by further independent internal or external review. As a result, the government did not have a good understanding of the cyber resilience of departments or specific IT systems. GSG used these limited and subjective data to estimate that 25% of government organisations were meeting the MCSS in 2022.

2.8 In April 2023, GSG started agreeing with departments clear and risk-based cyber resilience outcomes that they needed to achieve. It did this by introducing an annual cyber security assurance scheme, known as GovAssure, to objectively measure the cyber resilience of departments' IT systems against the National Cyber Security Centre's (NCSC) CAF (**Figure 3** overleaf). The CAF helps organisations show they have achieved appropriate cyber resilience outcomes based on the threat they face and the services they provide. To be cyber resilient, departments' critical IT systems need to meet one of two sets of outcomes created by GSG: 'baseline' or 'enhanced'.[5] GSG has jointly agreed with departments which set of outcomes they will use based on their role, likelihood of being targeted by a threat actor, IT estate and the level of risk they are prepared to take. This approach should help the government decide its priorities for investment more effectively, and track its progress in meeting the objectives of the Strategy. It also aligns government with best practice from the critical national infrastructure sectors.

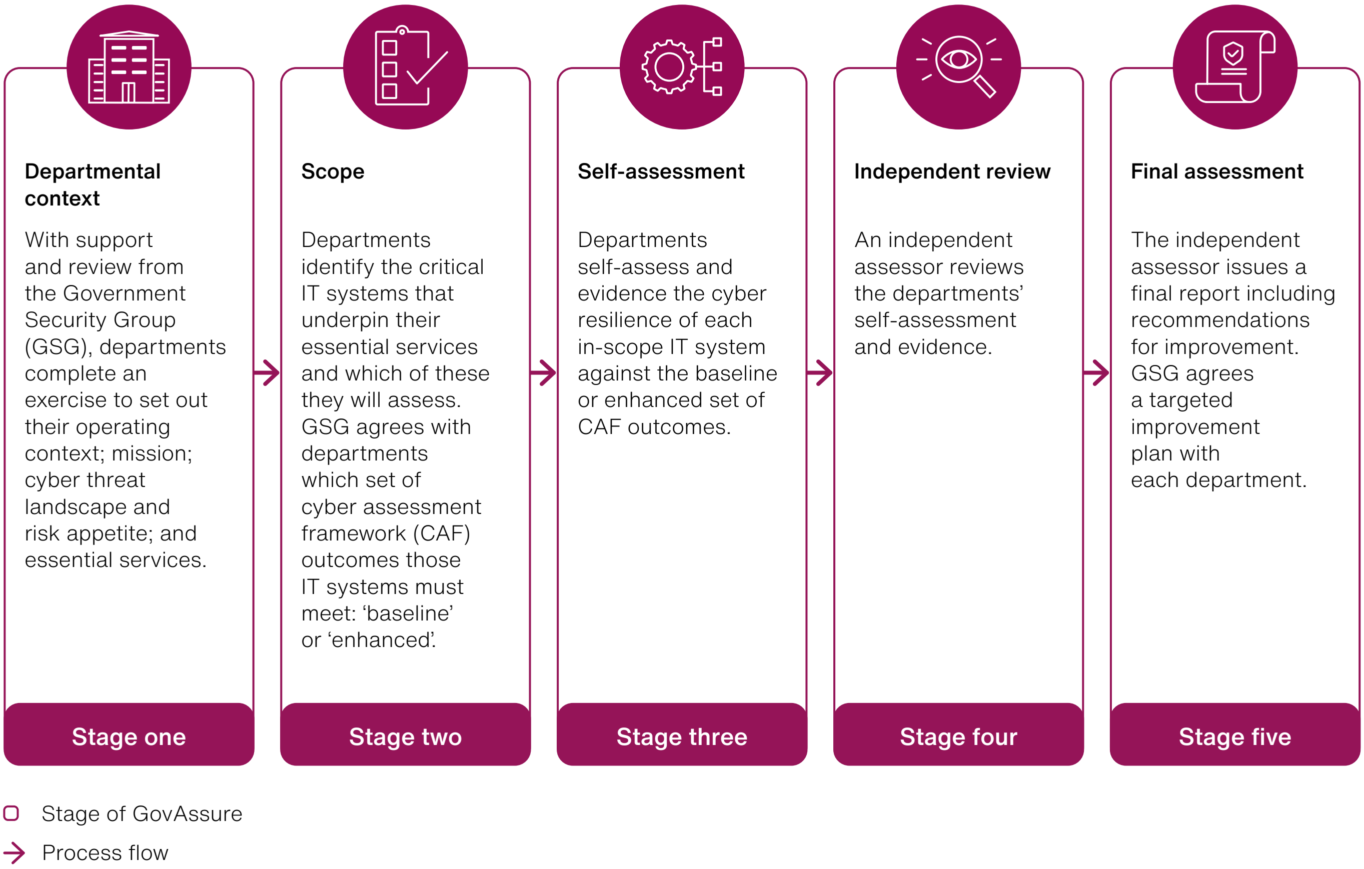
2.9 Between April 2023 and July 2024, GSG used GovAssure to begin collecting detailed, reliable data about how cyber resilient some of departments' most important IT systems are. It asked departments to use GovAssure to assess their cyber resilience and get independent reviewers to verify their performance. This method was more effective than previous approaches taken by government, which were based on more subjective self-reporting.

[5] GSG defines 'critical' IT systems as those that support a department's essential services. However, GSG excludes 'legacy' IT systems from this definition.

Figure 3

The 'GovAssure' cyber security assurance scheme, 2023 to 2024

GovAssure helps the government to identify and reliably assess the cyber resilience of departments' critical IT systems



Stage one

Departmental context

With support and review from the Government Security Group (GSG), departments complete an exercise to set out their operating context; mission; cyber threat landscape and risk appetite; and essential services.

Stage two

Scope

Departments identify the critical IT systems that underpin their essential services and which of these they will assess. GSG agrees with departments which set of cyber assessment framework (CAF) outcomes those IT systems must meet: 'baseline' or 'enhanced'.

Stage three

Self-assessment

Departments self-assess and evidence the cyber resilience of each in-scope IT system against the baseline or enhanced set of CAF outcomes.

Stage four

Independent review

An independent assessor reviews the departments' self-assessment and evidence.

Stage five

Final assessment

The independent assessor issues a final report including recommendations for improvement. GSG agrees a targeted improvement plan with each department.

□ Stage of GovAssure

→ Process flow

Notes

1 The Government Security Group (GSG) runs GovAssure annually; the first year took place between April 2023 and July 2024.

2 Departments can choose how many IT systems they will assess; they assessed a total of 72 systems in the first year.

3 GSG has not included 'legacy' IT systems within the scope of GovAssure.

Source: National Audit Office analysis of Government Security Group documents

2.10 GSG's other priorities, notably the need for GSG to respond to a cross-government cyber vulnerability, meant that:

- GSG launched GovAssure three months later than planned;
- GSG did not fully implement the findings of the GovAssure pilot before it began asking departments to start work on it;
- it offered less support to departments than it planned; and
- it needed to run GovAssure while still completing guidance for departments.

2.11 There was a further delay of four months as GSG did not receive assessments from all departments by its planned March 2024 end-date. GSG reported that departments' delays in submitting their assessments were because of their own cyber incidents and staff shortages. GSG plans to continue improving the GovAssure process. This includes short-term improvements, such as to guidance, and medium-term improvements, such as increasing automation to make GovAssure more efficient.

2.12 GSG and departments have lacked the time and resources to improve cyber resilience outcomes following the conclusion of the first year of GovAssure in July 2024. GovAssure has allowed GSG to identify priority issues and systemic vulnerabilities. For example, by August 2024, GSG had agreed targeted improvement plans (TIPs) with departments to remediate the priority issues identified through the GovAssure process. By November 2024, GSG had not commissioned progress updates from departments but planned to do so once departments had had more opportunity to implement their TIPs. Departments will not be able to confirm whether TIPs are fully funded until the 2025 Spending Review concludes.

Secure by Design

2.13 Working with industry, the Central Digital and Data Office (CDDO) has created an approach known as 'Secure by Design' (SbD). SbD aims for project teams and security professionals to use effective cyber security practices throughout the lifecycle of a digital service. It promotes a positive security culture and encourages cyber security to be everyone's collective responsibility. SbD could result in government organisations continually improving and maintaining their cyber resilience, as it will apply to all new services and significant changes to existing services.[6]

2.14 However, SbD is a long-term intervention and is unlikely to significantly contribute to the Strategy's aims for 2025 and 2030. CDDO plans to introduce the approach in stages until it is active across the public sector by 2026. Departments will be responsible for adopting the approach by meeting 10 principles, such as procuring technology securely and doing continuous assurance. It is too early to say how successful SbD will be, as it depends on departments' ability to uphold the SbD principles and on CDDO to incentivise and support compliance. Overall, in combination with the pace of GovAssure, this means that the government has not improved its cyber resilience quickly enough to meet the Strategy's aim for its core functions to be "significantly hardened" to cyber attack by 2025.

[6] 'Secure by Design' will apply to new services or changes to existing services with a value of over £100,000 (if public facing) or £1 million (for other digital services).

Strategic pillar two: Working in a coordinated and collaborative way to "defend as one"

2.15 The Strategy aims to enable government to be more collaborative and better coordinated so it can "defend as one" against the growing cyber threat. It aims to strengthen cyber defences by sharing threat intelligence, expertise and capabilities across organisations. We have previously reported that a failure to coordinate work to protect information across government meant that many bodies had overlapping mandates and activities. In October 2016, the government successfully consolidated four organisations into the NCSC, the UK's national technical authority.

2.16 The principle of "defend as one" is underpinned by GC3, which GSG established in September 2023 to better coordinate cyber security efforts across government. GC3 plans to do this by understanding, evaluating and sharing threat intelligence and vulnerabilities, and coordinating incident management. GC3 is a collaborative partnership between GSG, CDDO and the NCSC. GSG undertook a partial launch of GC3 services nine months later than planned because of its resource constraints. This means that GC3 has been providing its services while continuing to develop its governance, mandate and plans.

2.17 GC3 reported that it has started to have a positive impact, including by hosting a web-based form for cyber researchers to report vulnerabilities in government organisations and online services. The government has funded GC3 to 2025 using a combination of Cabinet Office operational budget and cyber transformation funding. GC3's planned work for 2025 is unlikely to meet the ambitions of GSG, CDDO and the NCSC because it has found it challenging to staff its work. The work of GC3 provides an opportunity for the centre of government to learn and build the business case for what a long-term, effective cyber operating model should look like.

2.18 However, departments still find it difficult to understand the roles of the different organisations at the centre of government that have cyber security responsibilities (**Figure 4** on pages 30 and 31). For instance, it is not always clear the extent to which the NCSC or GSG is responsible for government's cyber resilience and incident management. There are opportunities for GSG to improve how the centre of government communicates with departments, for example, in providing advice on the cyber threat and how to respond to it. Organisations at the centre also experience challenges in working together or raising awareness of what they can offer. For example, the Cyber Government Security Centre (GSeC), which GSG funds, has needed to initiate contact with departments to raise awareness of its free cyber security consultancy services. This is because there is not a centrally coordinated way of communicating GSeC's offer to departments to ensure that they seek it out when they need it. This could limit departments' take-up of those services.

2.19 In July 2024, the government announced that CDDO and the Government Digital Service (GDS) would move from the Cabinet Office to the Department for Science, Innovation & Technology. The government's intention is that this will bring together digital efforts to transform public services in one place. In January 2025, the cyber directorate of GSG remained located with other GSG directorates in the Cabinet Office, as part of the government security function. Regardless of how the government structures itself, there are still challenges for GSG and CDDO to overcome in how they coordinate to build cyber security into government's digital strategies and services.

GSG's progress towards making the public sector cyber resilient by 2030

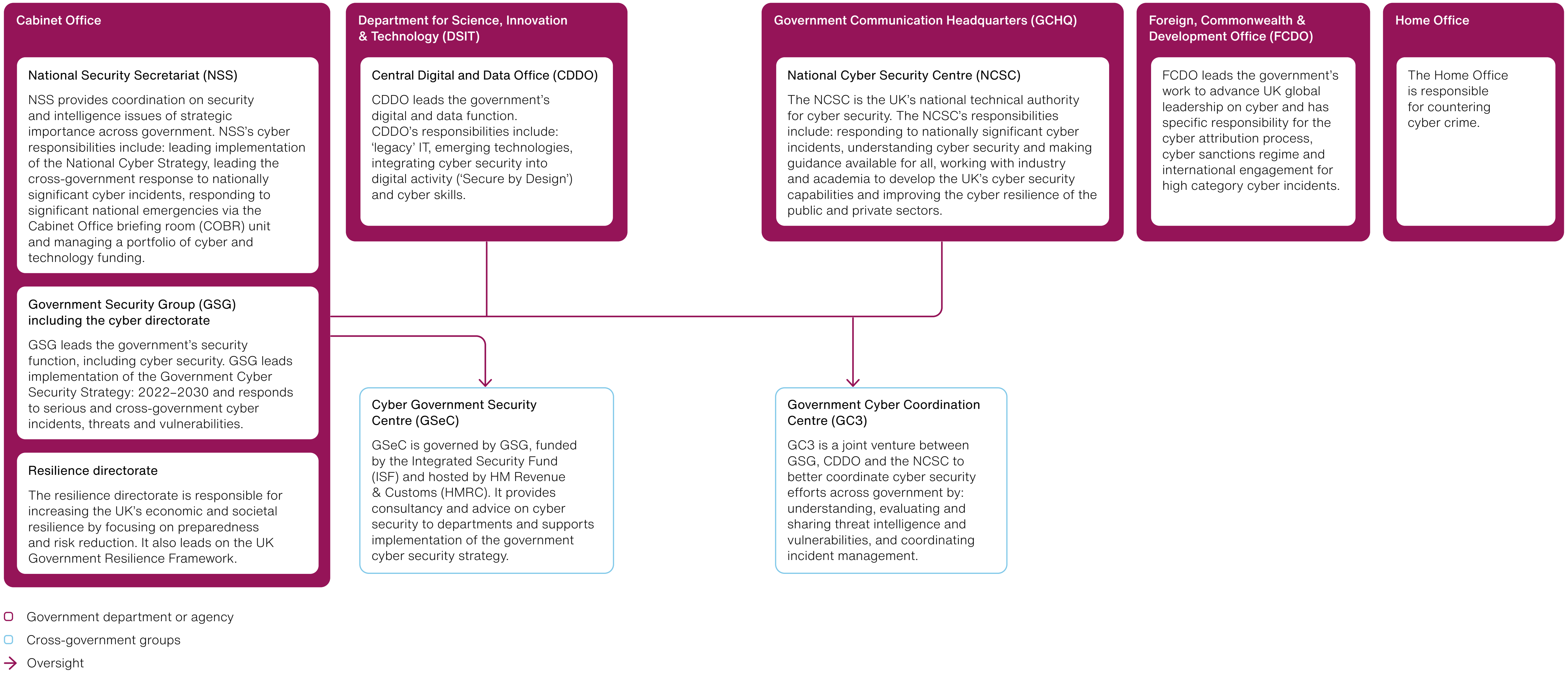
2.20 Good performance information helps identify how well an organisation is performing against its objectives and why. In March 2023, GSG agreed an interim set of metrics with the Government Security Board to measure progress towards the objectives of the Strategy. In July 2024, GSG started developing a more comprehensive monitoring and evaluation framework; this work was ongoing in November 2024. This means GSG has not yet been able to effectively measure, monitor and evaluate the government's progress or show how well its initiatives are working and why, other than through the GovAssure scheme which identified priority issues and vulnerabilities to government's cyber resilience (paragraph 2.12).

2.21 GSG assesses that making the public sector resilient to known vulnerabilities and attack methods by 2030 remains challenging. By January 2025, GSG had created an implementation plan describing the interventions it would make. However, GSG had not created a cross-government implementation plan setting out the role of departments. Making the public sector cyber resilient by 2030 will require cross-government effort, including by departments. A shared cross-government implementation plan would help clarify which parts of government need to do what and by when. GSG has not put robust arrangements in place to oversee how departments are implementing the Strategy because of its resource constraints. For instance, in April 2024, GSG asked departments to start developing their own implementation plans, but since then it has not asked departments for regular progress reports. GSG cannot track to what extent departments and their sectors are investing in cyber security.

Figure 4

The key organisations and teams at the centre of government with responsibilities for cyber security, January 2025

Many organisations and teams at the centre of government have responsibilities for cyber security



Cabinet Office

National Security Secretariat (NSS)

NSS provides coordination on security and intelligence issues of strategic importance across government. NSS's cyber responsibilities include: leading implementation of the National Cyber Strategy, leading the cross-government response to nationally significant cyber incidents, responding to significant national emergencies via the Cabinet Office briefing room (COBR) unit and managing a portfolio of cyber and technology funding.

Government Security Group (GSG) including the cyber directorate

GSG leads the government's security function, including cyber security. GSG leads implementation of the Government Cyber Security Strategy: 2022–2030 and responds to serious and cross-government cyber incidents, threats and vulnerabilities.

Resilience directorate

The resilience directorate is responsible for increasing the UK's economic and societal resilience by focusing on preparedness and risk reduction. It also leads on the UK Government Resilience Framework.

Department for Science, Innovation & Technology (DSIT)

Central Digital and Data Office (CDDO)

CDDO leads the government's digital and data function. CDDO's responsibilities include: 'legacy' IT, emerging technologies, integrating cyber security into digital activity ('Secure by Design') and cyber skills.

Government Communication Headquarters (GCHQ)

National Cyber Security Centre (NCSC)

The NCSC is the UK's national technical authority for cyber security. The NCSC's responsibilities include: responding to nationally significant cyber incidents, understanding cyber security and making guidance available for all, working with industry and academia to develop the UK's cyber security capabilities and improving the cyber resilience of the public and private sectors.

Foreign, Commonwealth & Development Office (FCDO)

FCDO leads the government's work to advance UK global leadership on cyber and has specific responsibility for the cyber attribution process, cyber sanctions regime and international engagement for high category cyber incidents.

Home Office

The Home Office is responsible for countering cyber crime.

Cyber Government Security Centre (GSeC)

GSeC is governed by GSG, funded by the Integrated Security Fund (ISF) and hosted by HM Revenue & Customs (HMRC). It provides consultancy and advice on cyber security to departments and supports implementation of the government cyber security strategy.

Government Cyber Coordination Centre (GC3)

GC3 is a joint venture between GSG, CDDO and the NCSC to better coordinate cyber security efforts across government by: understanding, evaluating and sharing threat intelligence and vulnerabilities, and coordinating incident management.

▢ Government department or agency

▢ Cross-government groups

→ Oversight

Notes

1 Other organisations and teams at the centre of government have a role in cyber security, such as the Joint Intelligence Organisation and the team leading 'Rosa', which is a government IT capability and service that enables working classified up to 'secret'. The Information Commissioner's Office also has a role in cyber security as the independent regulator for the protection of digital information.

2 The Integrated Security Fund (ISF) is a government-wide fund that addresses the highest-priority threats to UK national security.

3 In July 2024, the government moved the Central Digital and Data Office from the Cabinet Office to the Department for Science, Innovation & Technology.

Source: National Audit Office analysis of government documents

2.22 GSG oversees government security and helps develop good practice, which means it has offered support and guidance to departments, rather than mandating what they must do. In 2024, GSG began exploring how it might change how it works with departments to be more directive and to provide departments with more centralised capability and support. In April 2024, the Ministerial Cyber Board expressed support for the government taking a more centralised approach. GSG told us this could allow it to better manage and mitigate cyber risk to government, through centrally led cyber:

- assurance and response;
- services;
- technical standards and support; and
- skills (see paragraph 4.15).

2.23 GSG is learning from the experience of international partners who have taken a more centralised approach. For example, Australia provides cyber services at scale from the centre of government and uses technical teams to help departments. The UK centre of government provides some centralised cyber services, but these are spread across different organisations. For example, CDDO runs a service to make it easier for public sector organisations to secure their official internet domain name. The NCSC's 'active cyber defence' suite of services reduces the harm from basic, high-volume cyber attacks that affect people and government organisations' daily business. However, neither CDDO nor the NCSC are currently designed to provide services at scale to the rest of the government and the public sector in the long term.

Part Three

The government's cyber resilience position in 2024

3.1 The government defines cyber resilience as how well an organisation can continue running its most important business and services and ensure the protection of its data, despite adverse cyber security events. This part assesses the resilience of government organisations to the cyber threat they face.

The cyber resilience of departments' most important IT systems

3.2 Between April 2023 and July 2024, 35 government organisations took part in the first year of GovAssure. They self-assessed the cyber resilience of 72 IT systems they considered to be critical to running their essential services. The Government Security Group (GSG) has not tried to establish how many critical IT systems there are across the government's digital estate, but it considers that the assessed systems will be a small proportion of these. Most of the 35 organisations assessed between one and three of their critical IT systems against their agreed cyber assessment framework (CAF) outcomes. GSG plans that departments will continue to identify, document and assess their critical IT systems each year. Departments classified around two-thirds of the IT systems assessed as 'operational' (45 out of 72) and around one-quarter were 'enterprise' systems (17 out of 72). GSG required independent assessors to review all IT systems owned by lead government departments (those with responsibility for other public sector organisations) or that supported critical national infrastructure. Of the 72 IT systems assessed, independent assessors reviewed 58.

3.3 The 2024 data from GovAssure has allowed GSG to assess the gap between departments' actual and target levels of cyber resilience. It also showed that departments largely overestimated their level of cyber resilience, particularly those with lower cyber resilience maturity.

3.4 The 2024 GovAssure data of the 58 independently assessed critical IT systems showed significant gaps in government cyber resilience. The data highlighted multiple fundamental system controls that were at low levels of maturity across departments, including asset management, protective monitoring and response planning. In April 2024, GSG reported to ministers the implication of these findings: the cyber resilience risk to government was extremely high.

The cyber resilience of departments' legacy IT systems

3.5 'Legacy' IT is often more vulnerable to cyber attack and can be used as an entry point for threat actors to access and move across a network (see paragraph 1.3). In 2023, the government's Central Digital and Data Office (CDDO) published the legacy IT risk assessment framework, as part of its wider agenda to reduce departments use of outdated systems. CDDO uses this framework to collect data from departments on the number of legacy systems, departments' assessment of the likelihood and impact of operational and security risks occurring, and plans to remediate them.

3.6 In March 2024, CDDO identified that government departments had at least 228 legacy IT systems. Of these, CDDO assessed that:

- 28% of legacy systems (63 out of 228) were red-rated as there was a high likelihood and impact of risks occurring; and
- 72% of legacy systems (165 out of 228) were not red-rated, yet still presented a risk.

3.7 The data on legacy IT collected by CDDO relies on risk assessments provided by departments, which were not detailed and included aspects of cyber security in addition to other criteria. GSG did not include legacy systems in GovAssure because many of its recommended system controls would not be applicable to legacy systems. This means GSG does not have a detailed assessment of:

- the cyber security risks departments and their essential services are exposed to by using these legacy IT systems; or
- how well departments have managed this risk, for example, by isolating legacy systems from the rest of their network or performing vulnerability assessments.

Part Four

Challenges for departments in building cyber resilience

4.1 The centre of government and departments (including their arm's length bodies and delivery partners) share the responsibility for implementing the Government Cyber Security Strategy: 2022–2030 ('the Strategy'). This part assesses departments':

- ownership and accountability for cyber risk;
- performance in meeting their responsibilities; and
- investment decisions on cyber resilience.

Departments' ownership and accountability for cyber risk

4.2 Achieving the aims of the Strategy relies on departments managing their own cyber risk and that of the sectors for which they are responsible. Risk management is most effective when ownership of and accountability for risks are clear. The 2021 Government Functional Standard GovS 007: Security Standard (the Security Standard) sets expectations for the governance, roles and accountabilities, and practices needed for security, including cyber security.[7] It sets out that departments' accounting officers, who are accountable to Parliament, are responsible for making decisions that protect the security of their organisations.

4.3 Departments have not taken sufficient ownership or accountability for cyber resilience risk. Good practice emphasises the importance of leaders' ownership and accountability to ensure they deliver against their targets. Although departments' risk registers include major cyber and business resilience risks, it can be difficult to get leaders within departments to recognise how cyber risk is relevant to their strategic goals. In April 2024, the Government Security Group (GSG) recommended to the Ministerial Cyber Board that departments learn from best practice models of accountability and cyber risk management to improve their reporting on progress made towards meeting cyber resilience targets.

[7] The Security Standard is one of 15 functional standards (covering areas such as human resources, commercial and finance) that support consistent ways of working and accounting officers' stewardship of public resources.

4.4 The behaviour and actions of the board and the senior management team, particularly how they communicate with and challenge the business, reinforces the importance of risk management and encourages a consistent approach to safeguarding the business. Often, membership of departments' most senior decision-making boards and non-executive boards does not include any digital leaders or directors with cyber expertise. The government's July 2021 report, *Organising for Digital Delivery*, highlighted low technical fluency across senior civil service leadership as a challenge.[8] Officials working in departments in non-cyber roles, such as contract management, procurement, policy, or even digital, do not always consider the cyber security implications of their activities. This means they do not effectively manage, monitor or mitigate any cyber risks associated with their work.

Departments' performance in meeting their responsibilities in delivering the Strategy

4.5 The Strategy sets out the responsibilities of central government departments (a department controlled directly or indirectly by government ministers) including lead government departments (those with responsibility for other public sector organisations). This is to:

- manage their own cyber security risk;
- ensure their sectors and arm's-length bodies meet strategic resilience targets;
- assess and articulate the overall security position of wider public sector organisations, including arms-length bodies, agencies, local authorities and other public sector organisations;
- put in place appropriate governance arrangements to drive required improvement; and
- work collaboratively to address the collective issues.

Management of cyber risk of the most critical IT systems

4.6 In 2024, GovAssure data showed that multiple fundamental system controls were at low levels of maturity across departments, including asset management, protective monitoring and response planning (see paragraph 3.4). Departments' low level of maturity is likely to affect how well they could continue running if a successful cyber attack happened. Departments cannot manage risk effectively and make risk-based decisions about how they protect their most important assets, if they do not understand their digital estate and security risks.

[8] Digital Economy Council, *Organising for Digital Delivery*, July 2021.

4.7 Planning and 'exercising' an effective response are critical to minimising the impact of a cyber attack.[9] The Security Standard states that organisations should take steps to detect cyber attacks and aim to have a defined, planned and tested response to such incidents, especially when these affect sensitive information or key operational services. The National Cyber Security Centre (NCSC) can help departments to exercise their cyber incident response plans, although departments' use of this support is low.

Ensuring wider sectors are cyber resilient

4.8 In July 2023, GSG responded to an internal audit of the government security function's performance against the Security Standard, which identified an inconsistency in departments' oversight of their arm's-length bodies. In a paper to the Government Security Board, it set out plans to clarify its expectations for departments and arm's-length bodies. In April 2024, GSG reported it could not be confident that departments were meeting their responsibilities for ensuring their sectors and arm's-length bodies met resilience targets. GSG reported that it did not have a clear view of cyber resilience across the wider public sector. Many lead government departments had reported to GSG that they had insufficient funding, workforce and oversight mechanisms to understand and improve resilience across their sector.

Work collaboratively to address the collective issues

4.9 Some departments have been reluctant to share information about their cyber incidents with other parts of the government. This is a barrier to government achieving its aims for the "defend as one" strategic pillar. Sometimes, there are clear reasons for not sharing information. For instance, the information might be held at a high security classification, making it harder to share. When departments are transparent about their cyber incidents, however, other organisations can learn from them and improve their own cyber resilience. For example, in March 2024, the British Library published the lessons it had learned from its October 2023 cyber attack.[10] This was to ensure a "common level of understanding of key factors that may help peer institutions and other organisations learn lessons from the Library's experience".

The impact of investment decisions on cyber resilience

4.10 Departments' accounting officers are responsible for making decisions that protect the security of their organisations. In our report *Government resilience: extreme weather*, we said that government finds it challenging to make informed decisions about prioritisation to ensure efficient and effective investment in the long term.[11]

[9] A response plan should cover all relevant potential incidents. It should be auditable and testable (by 'exercising') across a range of incident scenarios.

[10] British Library, *Learning lessons from the cyber-attack*, March 2024.

[11] Comptroller and Auditor General, *Government resilience: extreme weather*, Session 2023-24, HC 314, National Audit Office, December 2023.

Investing in cyber security

4.11 In the 2021 Spending Review, the government announced it would invest £2.6 billion in cyber and 'legacy' IT, of which it allocated £1.3 billion to departments for cyber security and legacy IT remediation.[12] In January 2023, GSG reported that departments had funded the most urgent cyber priorities, but the ongoing Efficiencies and Savings Review and higher-than-expected inflation could affect further work. In July 2023, GSG reported that departments were at risk of not meeting their cyber resilience targets due to financial pressures. These included the potential need to absorb the cost of inflation within existing budgets and a lack of money for day-to-day operating costs (RDEL) to support infrastructure or equipment investment (CDEL).[13]

4.12 In April 2024, GSG reported to ministers that some departments had significantly reduced the scope of their cyber security improvement programmes to fund other priorities. It reported that the reasons for this included "cuts to programme funding, lack of access to cyber skills, challenges with delivery partners, and delays in departmental and cross government approvals". Ministers were concerned about the risk that departments were deprioritising cyber security funding.

Investing in legacy IT remediation

4.13 In 2022, half of departments told GSG that legacy IT was a critical risk to achieving their strategic resilience targets by 2025. Often, departments cannot meet their cyber resilience targets until they have invested in and carried out remediation work to keep legacy systems functional, secure and compliant. This might involve applying patches and security updates, or modernising and moving to cloud technologies. In March 2024, the Central Digital and Data Office (CDDO) identified that departments did not have fully funded plans to remediate around half of government's legacy IT assets (53%, or 120 out of 228), leaving these systems increasingly vulnerable to cyber attack. **Figure 5** shows that:

- departments had prioritised putting in place fully funded remediation plans for 78% of red-rated systems (49 out of 63);[14] and
- departments did not have fully funded remediation plans for 64% (106 out of 165) of the legacy systems that were not red-rated, yet still presented a risk.

[12] £1 billion was allocated to the National Cyber programme and £1.6 billion was announced for departments. However, in January 2023 a review of departmental spending concluded departments had been allocated £1.3 billion.

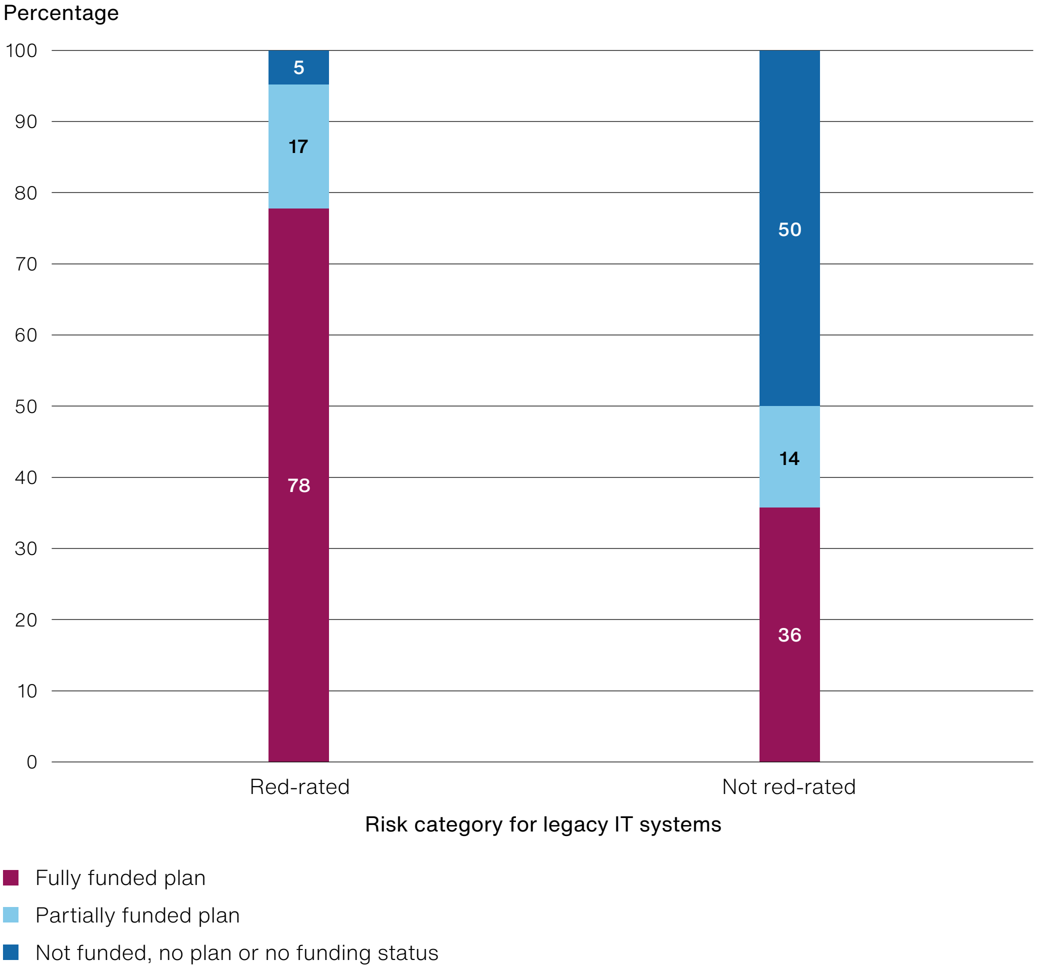
[13] Resource and capital delegated expenditure limits (RDEL and CDEL) are the limits set on departments' spending by HM Treasury.

[14] The Central Digital and Data Office (CDDO) categorises legacy IT systems as red-rated or not red-rated based on likelihood and impact of operational and security risks occurring.

Figure 5

The status of departments' plans to remediate 'legacy' IT systems, March 2024

Departments had fully funded plans to remediate more than three quarters (78%) of red-rated legacy IT systems, but did not have funded plans in place for many other legacy systems



Notes

1 'Legacy' refers to outdated computing software or hardware that is still in use.

2 The Central Digital and Data Office (CDDO) categorises legacy IT systems as red-rated or not red-rated based on likelihood and impact of operational and security risks occurring.

3 The data presented include 228 legacy IT systems, of which CDDO categorises 63 as red-rated and 165 as not red-rated.

4 The data do not include all legacy systems in central government. They are based on data provided to CDDO by 27 departments, which may not have identified all their legacy IT systems.

5 Remediation refers to addressing the risks posed by legacy systems, for example, by applying patches and security updates, or by modernising and moving to cloud technologies.

Source: National Audit Office analysis of Central Digital and Data Office data

Case study: how prioritisation decisions can impact the severity of a cyber attack when it occurs

4.14 In **Figure 6**, we set out the British Library's (the Library) experience of a cyber attack and the impact under-investment in its technology had on its severity. The Library identified the importance of "keeping infrastructure and applications up to date, with increased levels of lifecycle investment in technology infrastructure and security". The Library reported that it responded as quickly as it could and followed the necessary steps to limit the attack, but still suffered considerable damage.

Departments' cyber skills

4.15 Departments' cyber leaders report that attracting and retaining cyber skills in government organisations is one of the biggest risks to achieving their cyber resilience targets. For more than a decade, skilled cyber security professionals have been in short supply and high demand nationally and globally. Digital and technology leaders see the amount government organisations can pay, civil service recruitment processes, and external market conditions as the biggest barriers to recruitment and retention. In 2023-24:

- one in three cyber security roles in central government was either vacant or filled by temporary staff (contingent labour), costing, at a minimum, twice as much as permanent civil servants;
- the proportion of vacancies in several departments' cyber security teams was more than 50%, preventing core assurance functions from running effectively; and
- specialist roles were particularly difficult to recruit and 70% of security architects in post were temporary staff.

Figure 6
Case study: Ransomware attack on the British Library, October 2023

Ageing 'legacy' IT systems increased the severity of the cyber attack

What happened?

- The British Library (the Library) experienced a ransomware attack in October 2023.
- The Rhysida ransomware group claimed responsibility for the attack and demanded a ransom of 20 bitcoin, around £600,000 at the time, to restore services and return the stolen data.
- When the Library did not pay the ransom, Rhysida released around 600GB of stolen data online on the 'dark web'.

What was the impact?

- The impact on the Library's systems and services has been deep and extensive.
- The attack led to a leak of employee data and the Library's website being unavailable to users for almost a month. The attackers' methods included stealing and encrypting data and systems and destroying some servers to slow the Library's recovery and cover their tracks.
- The Library's efforts to rebuild its digital infrastructure started in December 2023 and was still ongoing in January 2025.
- The Library reported that the directly attributable additional costs resulting from the cyber attack totalled £600,000 by March 2024. The British Library told us that as its cyber recovery continues, the overall cost to it will be many times more than the costs incurred by March 2024.

Lessons learned on legacy IT remediation

- The Library had a diverse and complex technology estate, with many legacy IT systems.
- The Library kept some legacy applications longer than it originally intended. This made it harder for the Library to stay compliant with developing security standards.
- The Library assessed this contributed to the severity of the impact of the attack in three ways.
    1. Its legacy network design allowed the attackers wider access than would have been possible in a modern network design, allowing them to compromise more systems and services.
    2. Its use of older applications substantially increased the volume of customer and staff data on the network.
    3. Its reliance on legacy infrastructure increased the length of time that the Library required to recover from the attack. The Library will need to migrate, modify or even rebuild these legacy systems. This is because they cannot be repurchased or restored, or because they simply will not work on modern servers or with modern security controls.

Notes

1 'Legacy' refers to outdated computing software or hardware that is still in use.

2 The 'dark web' refers to parts of the internet that cannot be accessed by using traditional search engines.

Source: National Audit Office analysis of reports published by the British Library

4.16 Recruitment is fragmented across government. Some government organisations have been successful in attracting people with cyber skills, in part because of their departments' mission and cyber culture. Some organisations have developed their own cyber recruitment and training programmes based on their needs.[15] GSG has tried addressing the cyber security skills challenge in government by developing a cyber career framework, which it linked to a cyber learning curriculum and a cyber pay offer. However, it expects the cyber skills gap, between the skills it has and the skills it needs, will grow as departments increase their use of digital services and adopt new technologies to increase productivity. GSG's cyber skills initiatives that are available to departments include:

- a Cyber Apprentice Scheme (since 2020, GSG has recruited around 140 apprentices on behalf of 25 departments and, by June 2024, around 55 had graduated with a Level 4 cyber security technologist qualification);
- a Cyber Fast Stream programme (by November 2024, departments had recruited 37 individuals onto the programme); and
- the Government Cyber Security Academy, which since August 2024 has offered an accelerated training and recruitment pathway to non-experts.

4.17 Departments believe that the existing skills offer from the centre of government can overlap with their own, which can be inefficient and confusing. Additionally, some departments could not access cyber training programmes because of government caps on the number of civil servants that could be employed and recruitment freezes.

4.18 As part of its cyber skills programme, GSG has developed a government cyber skills strategy and a plan to reduce the government's cyber skills gap by 2030. In 2024, GSG assessed that, by 2030, there will be 751 cyber security vacancies in government, and that its skills interventions could fill 53% (399) of these if all its 19 skills interventions were fully funded. In January 2025, the government cyber skills strategy was partially funded. GSG is aiming to:

- attract and upskill cyber talent in government, for example, through its Government Cyber Skills Academy;
- retain cyber security civil servants, for example, by aligning to and obtaining professional titles set by the UK Cyber Security Council; and
- mature government's cyber security capability, for example, by providing cyber awareness training for all senior civil servants.

4.19 It is unlikely that GSG's plans will fully address the cyber skills gap. We have reported for more than a decade that previous government efforts to do so have not succeeded and it continues to find recruitment of cyber skilled people extremely challenging (see Appendix Three). The persistence of cyber skills shortages shows that the government may need to take a different approach to get the right cyber skills in government.

[15] The Department for Science, Innovation & Technology (DSIT) is responsible for improving the UK's cyber skills position.

Appendix One

Our audit approach

Introduction

1 This report examines whether the government's efforts to improve its cyber resilience are keeping pace with the cyber threat it faces. The report aims to hold government to account for its performance, increase transparency about how cyber resilient government is, and help government improve its cyber resilience.

2 Our scope includes the cyber resilience of ministerial and non-ministerial departments and their arm's-length bodies (all of which we refer to in this report as 'departments'). Our scope did not include the cyber resilience of local government, public corporations, businesses or UK society more widely. The report includes an example of a cyber attack on a supplier to the NHS, which demonstrates the effect cyber attacks can have on individuals. However, the scope of our fieldwork did not include assessing the cyber strategy or resilience of the NHS and adult social care. Additionally, our scope did not include the cyber security of departments' supply chains. This report focuses on the cyber resilience of IT systems at the 'official' level of security classification and not systems classified as 'secret' or above.

3 Throughout the report we refer to the centre of government. The centre of government is responsible for coordinating and overseeing the work of government, enabling it to achieve its strategic aims and ensuring there is a central view of the effective operation of the government as a whole. For the purposes of this report, we consider that this includes the Cabinet Office, HM Treasury, the National Cyber Security Centre (NCSC), the Central Digital and Data Office (CDDO) as well as cross-government functions such as the security function, and the digital, data and technology function.

4 We conducted our fieldwork between May and October 2024. We used the results of this work to inform the findings, conclusions and recommendations of this report.

Our evidence base

Methods

Interviews

5 We interviewed key officials from the Cabinet Office to understand how they had designed and begun to support departments to implement the Government Cyber Security Strategy: 2022–2030 ('the Strategy'), and how they worked with departments and other stakeholders to better achieve the government's objectives. Those we interviewed included:

- senior officials responsible for leading the Government Security Group (GSG);
- officials responsible for implementing the Strategy;
- officials responsible for national security policy; and
- officials involved with threat assessment and incident response.

6 We also interviewed other officials from central government, including:

- senior officials from the NCSC, to discuss the role of the NCSC as the national technical authority for cyber security;
- officials from CDDO, to understand the links between government's wider digital ambitions and its management of the government's legacy IT estate and cyber security risks; and
- officials from the government's central risk and resilience functions, to understand how they consider cyber risks.

7 To understand the perspectives of spending departments in dealing with cyber risk on a day-to-day basis, we also interviewed senior cyber security officials from the following organisations:

- HM Revenue & Customs;
- the Department for Work & Pensions;
- the Home Office;
- the Ministry of Housing, Communities & Local Government;
- the Ministry of Justice; and
- the British Library.

8 We did not design these interviews to represent a statistically significant group. Instead, we undertook them to triangulate the evidence from central government with a range of views from those with practical experience of implementing different approaches to cyber resilience in their organisations.

9 Our final interviews were with other stakeholders from the sector to better understand issues around skills and culture. These included one member from each of the government's National Cyber Advisory Board and the UK Cyber Security Council.

10 Overall, we conducted 42 interviews over our fieldwork period. These were a mix of face-to-face and remote interviews conducted over Microsoft Teams. We selected most interviewees based on discussions with GSG, but selected others during our fieldwork in response to new information. As well as undertaking these targeted interviews, we also drew on recent evidence from National Audit Office engagements with other departments.

11 We summarised the content of our interviews thematically based on the study questions that we used in the report. We used this analysis to identify and support our key findings and recommendations.

Document and data review

12 We reviewed published and unpublished documents and data from the Cabinet Office to understand how the government is managing cyber resilience. These sources included:

- ministerial submissions setting out the extent of the cyber resilience challenge;
- assessments of the threats to cyber resilience from a range of actors;
- data and analysis underpinning the results of the GovAssure process; and
- management documents setting out progress with the Strategy.

13 We reviewed documents between June and October 2024. We tagged the documents with the area of the report to which they related, and we extracted information relevant to the study questions that we used in the report. We also made use of team discussions to identify emerging findings following our review of documents.

Appendix Two

Examples of cyber attacks on public bodies

1 **Figure 7** shows examples of how publicly reported cyber attacks have affected government departments and public bodies in recent years, including the Ministry of Defence, NHS England, the Electoral Commission and Parliament.

Figure 7

Examples of cyber attacks on public bodies between 2021 and 2024

Public bodies have experienced a range of cyber incidents

Affected body	Date	Nature of cyber incident	Impact
Ministry of Defence (MoD)	May 2024	MoD's payroll contractor's network was compromised by a malicious cyber actor. This network held armed forces staff members' data.	The data at risk was an estimated 270,000 payroll records belonging to members of Britain's armed forces. These records included names and bank details, and in a small proportion of cases, addresses and National Insurance numbers of serving and former members of the Army, Royal Navy and Royal Air Force and reservists.
NHS England and several local authorities	March 2023	Capita, the government's largest IT contractor, experienced a cyber attack where the intruder gained unauthorised access to data.	NHS England and several local authorities reported that personal data of patients and residents were accessed. The extent of the wider impact on government was unclear.
Electoral Commission	2021-22	The compromise of computer systems at the UK Electoral Commission between 2021 and 2022 has been attributed to a China state-affiliated actor.	The National Cyber Security Centre (NCSC) assesses it is highly likely the threat actors accessed and exfiltrated email data, and data from the Electoral Register during this time, which in combination with other data sources would highly likely be used by the Chinese intelligence services. Since the compromise, the Electoral Commission has implemented a multi-level security system, and improved resilience and monitoring, through significant investment. The Information Commissioner's Office confirmed that the Electoral Commission has now taken the necessary steps to improve its security.
Parliament	2021	A China state-affiliated cyber actor was highly likely responsible for a cyber campaign against the parliamentary email accounts of members across both Houses of Parliament.	Parliament's security department identified and mitigated the cyber campaign before it could compromise any accounts.

Note

1 State-affiliated actors include those who are funded by states and governments.

Source: National Audit Office analysis of publicly available information

Appendix Three

Long-standing digital and cyber skills challenges

1 We have reported for more than a decade that previous government efforts to deploy suitably qualified and experienced digital and cyber security professionals have not succeeded and that the government continues to find recruitment of those people extremely challenging (**Figure 8**).

Figure 8

Our previous findings on the digital skills challenge, 2011 to 2023

We have consistently reported that the government has not successfully addressed the gap between the digital skills it has and the digital skills needed

Year	Report	Finding
2011	*Implementing the Government ICT strategy: six-month review of progress*	The government has not established a baseline requirement for ICT professional resources across central government or filled key immediate skills gaps.
2013	*The impact of government's ICT savings initiatives*	Digital skills remain a challenge across government, with capacity and capability gaps appearing across central government.
2015	*The digital skills gap in government: Survey findings*	Recruitment, market conditions and procurement processes were all still significant challenges. Initiatives go some way to delivering the skills needed, but there are broader, systemic issues to tackle. We questioned whether there was realism about the scale and pace of transformation achievable within the available resources and skills.
2021	*The challenges in implementing digital change*	Many departments face a large capacity gap for people with digital skills. There is a global shortage of digital skills, which makes this challenging to overcome.
2022	*The Digital Strategy for Defence: A review of early implementation*	The Ministry of Defence (MoD) does not have enough people with the right digital skills. Although MoD has tried to address this, it has not made fast enough progress to match the problem and needs a different approach.
2023	*Digital transformation in government: addressing the barriers to efficiency*	Progress in improving the digital capability of senior decision-makers in government has been limited. Additionally, the activities set out in government's roadmap do not fully address the reality that the government cannot easily fill its digital vacancies and skills gaps.

Source: National Audit Office analysis of its reports referencing the digital skills challenge, 2011 to 2023

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: 014935-001

£10.00
ISBN: 978-1-78604-595-9