INSIGHT

Cyber security and resilience

National Audit Office

Good practice guidance

October 2025

Our insights products provide valuable and practical insights on how public services can be improved. We draw these from our extensive work focused on the issues that are a priority for government, where we observe both innovations and recurring issues. Our good practice guides make it easier for others to understand and apply the lessons from our work.

We are the UK's independent public spending watchdog

DP Ref: 017033

Insights

Our insights products provide valuable and practical insights on how public services can be improved. We draw these from our extensive work focused on the issues that are a priority for government, where we observe both innovations and recurring issues. Our good practice guides make it easier for others to understand and apply the lessons from our work.

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 2024, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £5.3 billion. This represents around £53 for every pound of our net expenditure.

Contents

Introduction

The cyber security landscape has evolved significantly since the publication of our previous guide for audit and risk assurance committees in 2021. Hybrid working is now the norm, with people accessing corporate data from a range of locations and devices. Many organisations are increasingly reliant on cloud-based systems accessed over the internet as traditional on-premises installations are being phased out. Our ability to work online has also become more unpredictable, with highly capable state and state-aligned actors using increasingly sophisticated methods to conduct malicious cyber activity.

Cyber security is the practice of protecting systems, networks, devices and data from digital attacks, to ensure the confidentiality, integrity and availability of information. Cyber resilience refers to the ability of an organisation to maintain the delivery of its key functions and services and protect its data in the face of an adverse cyber event.

Despite the UK government prioritising cyber security and resilience for over a decade, our January 2025 report on *Government cyber resilience* identified that the government's cyber resilience levels are lower than previously estimated. The threat landscape is rapidly escalating, yet significant gaps persist in critical areas.

This guide is for audit and risk assurance committees and non-executive directors. Our goal is to support their scrutiny and challenge by understanding and addressing the key questions necessary for reducing cyber risk and achieving cyber resilience. While aspects of cyber security can be complex, it is not solely a technical issue about products and services. The non-technical aspects such as governance, policies, processes, training and exercises are just as important. Effective oversight does not require deep technical expertise. Rather, it depends on asking the right questions, fostering a culture of accountability, and ensuring collaboration between audit committees, senior leaders and technical teams.

Why this issue requires attention

Cyber-attacks continue to have serious consequences for government organisations, public services and people's lives. The *Government Cyber Security Strategy: 2022 to 2030* highlights that government organisations are "routinely and relentlessly targeted" by malicious actors. Although there is no single source of data to quantify the cyber threat to the public sector or government IT systems, the National Cyber Security Centre (NCSC) reported that 40% of the incidents it managed between September 2020 and August 2021 targeted the public sector.[1] This includes local government, central government and the devolved administrations, as well as political parties, intelligence, emergency and health services, and law enforcement.

Recovery can be prolonged and costly, as evidenced by the extensive impact of the October 2023 cyber-attack on the British Library. The incident resulted in the encryption and destruction of a significant portion of the library's server infrastructure, as well as the theft and online auction of a substantial amount of user and staff data.

The library's infrastructure rebuild and service restoration efforts have been extensive, with ongoing service disruptions over a year later. The severity of the attack was exacerbated by an historic under-investment in legacy technology and cyber security.

Additionally, the government faces significant challenges in attracting and retaining individuals with cyber skills, as well as in enhancing the capabilities of its current workforce. For over a decade, there has been a national and global shortage of skilled cyber security professionals, coupled with a high demand for their expertise.

Why audit committees need to monitor cyber risks

Cyber risk poses significant threats to operational continuity, public trust and financial integrity. Audit and risk assurance committees have a critical role in assuring that appropriate controls, governance and resilience measures are in place and working effectively.

Audit and risk assurance committees need to know enough about cyber security and the associated risks to effectively perform their challenge and oversight roles. This is particularly crucial in a fiscally constrained environment where threats are evolving faster than the government's ability to keep pace.

1 While the NCSC provides incident insights and thematic assessments, it had not published a unified statistical analysis of cyber threats to the public sector as at the time this guide was written.

Continued Introduction

How government policy has changed in this area

Since our last guide was published, the government's approach to cyber security has evolved. The *Government Cyber Security Strategy: 2022 to 2030* is the first strategy that focuses only on the government's cyber resilience, rather than that of the UK economy more widely. Its definition of government includes departments, arm's-length bodies, agencies and local authorities, recognising that many diverse public sector organisations deliver core government functions. The strategy set a target for all government organisations across the whole public sector to be resilient to known vulnerabilities and attack methods by no later than 2030.

The *UK Government Resilience Action Plan* published in July 2025 sets out the strategic intent and approach to national resilience. It includes an objective to "develop a comprehensive national resilience assessment". This will involve creating a new data-driven resilience baseline, alongside a Cyber Resilience Index focused on Critical National Infrastructure.

This will be particularly relevant to departments with operational responsibility for, or oversight of, elements of the UK's Critical National Infrastructure.

Under previous arrangements, although departments were required to meet the government's minimum cyber security standard, they had the freedom to assess which additional service and organisational standards or frameworks (for example, ISO 27001, NIST) they wished to adopt, as well as how they would be evaluated and assured. Departmental security health checks were based on self-assessment and did not require validation through independent internal or external reviews. Yet, by 2022, the Cabinet Office estimated that only a quarter of government organisations had met the minimum standard.

The cyber security elements of the departmental security health checks were replaced in April 2023 by a new assurance regime called GovAssure. This focuses on the critical systems that support an organisation's essential services, rather than on conducting a more general entity-wide health check. Systems are assessed against either a 'baseline' or 'enhanced' profile based on the NCSC's Cyber Assessment Framework.

A key feature of GovAssure is that the results and supporting evidence are subject to review by an accredited independent assessor. The outcome is a targeted improvement plan, although organisations must fund work under the plan from their own resources. See Appendix One for more information.

Alongside GovAssure, in 2024, the government introduced Secure by Design as an approach for future systems implementations. This comprises a set of 10 principles aimed at building security into digital services and their underlying technical infrastructure. It is applicable to both in-house and externally acquired or developed systems and services. While Secure by Design is not retrospective, it applies to significant changes to existing services as well as to new services.

It is mandatory for central government departments and arm's-length bodies and recommended for the wider public sector. Further details can be found in Appendix Two.

Neither GovAssure nor Secure by Design is being applied to legacy systems that expose government to high levels of cyber risk. The expectation remains that these are assessed and ranked for remediation according to the existing Legacy IT Risk Assessment Framework first published in September 2023. This is summarised in Appendix Three.

Continued Introduction

What we have found

Our January 2025 report on *Government cyber resilience* highlighted that the government's efforts to enhance cyber resilience are being outpaced by the evolving threat landscape. The extensive size, age and variety of the government's digital assets pose significant challenges to achieving cyber resilience.

Despite improvements in coordination, we found departments still struggle to understand the roles and responsibilities of cyber organisations within the government. There are also inadequate measures to assess the effectiveness of efforts to bolster cyber security.

The first year of GovAssure revealed considerable gaps in the cyber resilience of departments. We found that they have not fulfilled their obligations to enhance both their own and the broader sector's cyber resilience. Competing priorities and financial constraints have limited the scope of cyber security initiatives.

Furthermore, significant challenges remain in recruiting and retaining personnel with cyber skills and in providing upskilling opportunities.

These findings are echoed in the *State of digital government review* published in January 2025 by the Department for Science, Innovation and Technology (DSIT). The review warns that cyber risk to the government is critically high, yet public organisations are under-prepared for current and evolving threats.

The continued prevalence of legacy technology is a factor, and half of the organisations across central and local government and the emergency services surveyed for the review reported that, when there is a budget for legacy system remediation, it frequently gets reallocated to other initiatives.

Our guidance

How this guidance links to other publications

This guidance sets out to supplement existing standards and government guidance, rather than to replace or rewrite them.

Drawing from government cyber security guidelines and our experience with the organisations we audit, the following sections are designed to help audit committees tackle both strategic and critical operational issues. The goal is to ensure that the broader context of each issue is clear and that the questions posed highlight key areas of focus.

What this guidance covers

This guide covers cyber security and resilience, which the government defines as follows.

- **Cyber security** is the protection of systems (including hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
- **Cyber resilience** is the ability of an organisation to maintain the delivery of its key functions and services and to ensure the protection of its data, despite adverse cyber security events.

Effective measures to reduce cyber risk rely on people and the management of processes as well as technical controls. They are an integral part of the wider activity of information security, which encompasses electronic, physical and behavioural threats to an organisation's systems and data. They also play a part in supporting organisational resilience.

High-level questions

In engaging with management to explore the maturity of cyber security and resilience, audit and risk assurance committees may wish to consider various high level issues first before discussing points of detail or technical activity. The questions below are based on the essentials we believe need to be addressed and are consistent with the *Cyber Governance Code of Practice* published in April 2025 by the NCSC and DSIT.

The questions are aimed at those with an oversight role rather than being involved with day-to-day management of cyber security. Overall, management should be able to describe to their boards a balanced approach which considers people (culture, behaviours and skills), process, technology and governance to ensure a flexible and resilient cyber security response.

Continued
Our Guidance

Question 1:
Strategy

- Is there a clear and effective cyber strategy as part of the overall business strategy, setting out the high-level actions to improve the organisation's resilience?
- Are all business areas clear about their cyber security obligations and responsibilities, and resourced and empowered to implement good cyber security measures?
- Is sufficient funding prioritised and protected in order to match the intent of the strategy?
- Does the organisation understand and comply with legislative requirements, for example data protection and applicable government policies and standards?

Question 2:
Assurance and oversight

- Does the organisation receive regular threat briefings and assessments from NCSC and other industry partners and does this inform the risk assessment?
- Are regular threat assessments undertaken, including representatives from across the business and the supply chain, and are unacceptable risks escalated?
- Is there regular formal reporting into the most senior decision-making body on at least a quarterly basis tracking risk tolerances and providing oversight of strategic delivery?
- Are roles and responsibilities clearly understood?
- Does the organisation obtain assurance over the cyber security posture of critical suppliers and partners?
- Do governance structures ensure compliance is monitored and reported effectively?
- Is the 'second line of defence' adequately resourced with sufficient expertise to provide independent challenge and oversee cyber security and resilience effectively?
- Does reporting provide meaningful insight rather than just technical detail?
- Does reporting explicitly link back to strategy and risk?

Question 3:
Risk management

- Have the systems, data, software, services and networks which are critical to the organisation's objectives been identified and classified by sensitivity and criticality?
- Is cyber security risk integrated into and considered as part of the overall approach to risk management and considered in strategic decision making?
- Is a cyber risk register in place, with clear owners, actions and escalation mechanisms?
- Has the organisation defined and communicated its cyber risk appetite and tolerance levels, and if so, are these integrated into decision making, investment, and mitigation plans?
- Is there a structured method or framework for managing risk that fits the organisation's business and technology needs, for example ISO/IEC 27001, 27005, NCSC Cyber Assessment Framework (CAF), noting that government departments and arm's-length bodies are mandated to meet or exceed the security outcomes specified in the appropriate CAF profile (baseline or enhanced) for their critical systems?
- Are cyber risks regularly reviewed in line with the evolving threat landscape, and does this include those arising from newer technologies, such as developments in artificial intelligence, cloud computing and cloud-native architecture?
- Has the organisation gained assurance over the cyber security of its commercial partners and suppliers of products and services, including through contractual obligations, audits or certifications? (At a minimum, all government suppliers holding OFFICIAL data should hold a valid Cyber Essentials Certificate or equivalent in accordance with the Procurement Policy Note on the Cyber Essentials Scheme.)[1]

Question 4:
People

- Are board members fully aware of their responsibilities for cyber governance, and have they received appropriate training?
- Does the organisation foster a positive cyber security culture, with the appropriate tone set from the top?
- Is there clear executive accountability for cyber security, and is this responsibility cascaded across the organisation?
- Has a baseline assessment of the organisation's current cyber expertise been conducted, identifying gaps and areas of weakness?
- Is there a structured programme to ensure that all staff have at least a basic level of cyber awareness?
- Is there regular evaluation of the effectiveness of cyber awareness initiatives (for example phishing simulations)?

1 Cabinet Office, *Procurement Policy Note: Cyber Essentials Scheme*, updated February 2025, available at https://assets.publishing.service.gov.uk/media/67af78c8a75f02dffca29bd8/PPN_014_Cyber_essentials_scheme.pdf

Continued
Our Guidance

- Are third-party contractors and temporary staff included in cyber awareness and training programmes?
- Is there a plan in place to develop or obtain access to the cyber security skills and expertise the organisation needs?
- Are cyber policies developed collaboratively with relevant departments (for example, human resources) and clearly communicated across the organisation?
- Is there a simple and trusted process for reporting cyber incidents or concerns, and a culture where staff feel confident to do so?
- Does the organisation regularly reassess its resilience plans against known breaches reported by other organisations?

Question 5:
Incident planning, response and recovery

- Does the organisation have a well-prepared and tested cyber incident response plan aligned with its risk appetite and business continuity priorities?
- Is the plan regularly exercised for likely scenarios and updated for lessons learned?
- Does the organisation have clarity on the sources of external support (for example, legal, technical, communications) available during a major incident, and are these integrated into the response plan?
- Have lessons been learned from past incidents or near misses, and have they informed improvements?
- Is there sufficient monitoring and logging in place to identify a potential intruder or attack, and are the warnings promptly acted upon?
- Is there an adequate data and asset backup strategy in place?
- Are controls in place to protect backups from being compromised or destroyed during an attack?

More detailed areas to explore

Legacy systems

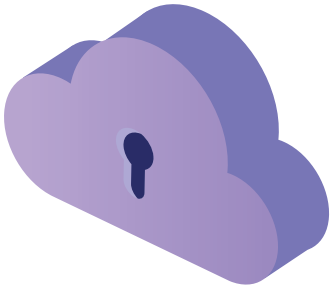
- Have all legacy systems been identified and catalogued?
- Have they been evaluated against the Legacy IT Risk Assessment Framework?
- For systems rated ‘red’ under the Framework, is there a remediation plan with a firm target date by which remediation is expected to be completed?
- Is funding for the plan secured for its entire duration?
- Is the funding ring-fenced or otherwise ‘protected’ against being diverted to unrelated purposes?
- Is implementation being monitored?
- Are ongoing maintenance costs factored into business cases and budget submissions?

GovAssure

- Have the critical systems essential to the delivery of the core purpose of the organisation been identified and prioritised for GovAssure?
- Has a targeted improvement plan been agreed for systems already assessed?
- Is the targeted improvement plan adequately funded?
- Is the funding ring-fenced or otherwise ‘protected’ against being diverted to unrelated purposes?
- Is implementation of the improvements being monitored?
- Is there an effective way to deal with issues encountered during implementation?

Secure by Design

- Have the principles been adopted for all future systems developments and procurements?
- Are commercial partners and suppliers clear on their obligations?
- Do contractual arrangements mirror that commercial clarity?



Further resources

Government strategies and guidance

- Cabinet Office, Government Cyber Security Strategy: 2022 to 2030 (2022) *https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030*
- Government Functional Standard GovS 007: Security (2021) *https://www.gov.uk/government/publications/government-functional standard-govs-007-security*
- Department for Science, Innovation and Technology and NCSC, Cyber Governance Code of Practice (2025) *https://www.gov.uk/government/publications/cyber-governance-code-of-practice*
- National Cyber Security Centre (NCSC), 10 Steps to Cyber Security (2021) *https://www.ncsc.gov.uk/collection/10-steps*
- NCSC, Cyber Security Toolkit for Boards *https://www.ncsc.gov.uk/cyber-governance-for-boards/toolkit*
- NCSC, Cyber Assessment Framework (2024) *https://www.ncsc.gov.uk/collection/cyber-assessment-framework*
- NCSC, Cyber Essentials *https://www.ncsc.gov.uk/cyberessentials/overview*
- Government Security, GovAssure (see Appendix One) *https://www.security.gov.uk/policy-and-guidance/govassure*
- Government Security, Secure by Design (see Appendix Two) *https://www.security.gov.uk/policy-and-guidance/secure-by-design*
- Government Digital Service and Central Digital and Data Office, Guidance on the Legacy IT Risk Assessment Framework (see Appendix Three) *https://www.gov.uk/government/publications/guidance-on-the-legacy-it-riskassessment-framework*

National Audit Office reports and insights

- Government cyber resilience (January 2025) *https://www.nao.org.uk/reports/government-cyber-resilience*
- Guidance for audit committees on cloud services (September 2024) *https://www.nao.org.uk/insights/guidance-for-audit-committees-on-cloud-services-2*
- Digital transformation in government: a guide for senior leaders and audit and risk committees (February 2024) *https://www.nao.org.uk/insights/digital-transformation-in-government-a-guide-for-senior-leaders-and-audit-and-risk-committees*
- Audit and Risk Assurance Committee effectiveness tool (May 2022) *https://www.nao.org.uk/insights/audit-and-risk-assurance-committee-effectivenesstool*
- Overcoming challenges to managing risks in government (February 2025) *https://www.nao.org.uk/insights/overcoming-challenges-to-managing-risks-in-government*

Appendix One

GovAssure

In April 2023, the government introduced GovAssure as an annual cyber security assurance scheme to objectively measure the cyber resilience of departments' systems against the National Cyber Security Centre's Cyber Assessment Framework (CAF). 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 systems need to meet one of two sets of outcomes: 'baseline' or 'enhanced'. The central Government Security Group (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. (The details of the baseline and enhanced profiles are not in the public domain, so we do not describe them further here.)

This approach is intended to help the government decide its priorities for investment more effectively and track its progress in meeting the objectives of the *Government Cyber Security Strategy: 2022 to 2030*. It also aligns the government with best practice from the critical national infrastructure sectors.

There are five stages to the GovAssure process.

1. **Departmental context:** With support and review from GSG, departments complete an exercise to set out their operating context, mission, cyber threat landscape and risk appetite, and essential services.
2. **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 outcomes those IT systems must meet: 'baseline' or 'enhanced'.
3. **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.
4. **Independent review:** An independent assessor reviews the departments' self assessment and evidence.
5. **Final assessment:** The independent assessor issues a final report that includes recommendations for improvement. GSG agrees a targeted improvement plan with each department.

Appendix Two

Secure by Design

The Government Digital Service has developed the Secure by Design approach in collaboration with industry. This initiative aims to integrate effective cyber security practices throughout the lifecycle of digital services, fostering a positive security culture and making cyber security a collective responsibility.

Secure by Design is a set of 10 principles aimed at ensuring the security of digital services and their underlying technical infrastructure. It applies to the development, procurement and contracting of new systems. It does not apply to existing legacy systems, as retroactive application was deemed impractical.

It is mandatory for central government organisations and arm's-length bodies, and optional for the wider public sector. Commercial partners are also expected to understand and comply with these requirements as they flow down the supply chain.

The ten principles are as follows:

1. **Create responsibility for cyber security risk:** This is about assigning senior stakeholders with sufficient experience, knowledge and authority on security matters to be accountable for managing the cyber security risks for a service.
2. **Source secure technology products:** There should be sufficient due diligence to consider security vulnerabilities when using third-party products.
3. **Adopt a risk-driven approach:** This is about assessing cyber security risks to build in appropriate protections to address the evolving threats.
4. **Design usable security controls:** These must be fit for purpose and easy to understand.
5. **Build in 'detect and respond' mechanisms:** This recognises that security incidents are inevitable, therefore appropriate monitoring, alerting and response capabilities should be integrated into the service and regularly tested and iterated.
6. **Design flexible architectures:** These should allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities.
7. **Minimise the attack surface:** This means using only the minimum necessary technology capabilities to provide a service.
8. **Defend in depth:** This is about creating layers to make it harder for an attacker to compromise a system if a single control is overcome.
9. **Embed continuous assurance:** This should provide ongoing confidence in the effectiveness of security controls.
10. **Make changes securely:** This means ensuring the security impact of changes is considered along with other factors.

Appendix Three

Legacy IT Risk Assessment Framework

The Legacy IT Risk Assessment Framework provides a structured approach for evaluating and prioritising the risks associated with outdated IT systems within government departments. By systematically assessing the likelihood and impact of system issues, departments can make informed decisions to mitigate risks, enhance operational efficiency, and contribute to the broader goals of modernisation and digital transformation.

The framework uses two categories of criteria: likelihood and impact. Each category is further divided into specific criteria to provide a comprehensive assessment of risk levels. To effectively use the framework, organisations should start by identifying the specific IT system and its components, including hardware, software, and support contracts. This system is then scored against each of the likelihood and impact factors to reflect the probability of each factor occurring over a three-year period, and the potential impact based on the severity and scope of the consequences. The overall scores from both likelihood and impact criteria are aggregated by finding the average of the mean of the scores and the maximum score, resulting in an overall risk score.

Systems with an overall risk score of 16 or above are considered 'red-rated', indicating a nationally critical level of risk requiring immediate attention. Such 'red rated' systems should be prioritised for urgent modernisation, updates or replacement, while addressing lower-risk systems in subsequent phases.

Likelihood factors

This is used to assess the chance of system issues, such as a failure, being realised. The following factors are scored on a scale from 1 to 6 (where 1 is very low, 5 is very high and 6 is certain).

- The technology used is out of support, i.e. technical support, upgrades, patches, and new features.
- Support contracts for services are due to expire with no replacement agreement.
- Prevalence of personnel with skills and knowledge to provide support and make changes to the asset.
- Technical inability for asset to meet current or future business needs (for example, inability to be scaled or have improvements applied).
- The asset is based on old hardware or housed in improper physical environment (for example, due to climate, location).
- Security vulnerabilities.
- Evidence of historical failures or issues.

Impact factors

This covers the impact resulting directly or indirectly from system issues, for instance failure or attack. The following factors are scored on a scale from 1 to 5 (where 1 is very low and 5 is very high).

- Impact of a failure of the system directly or indirectly resulting in a threat to national security, health, personal safety or loss of human life.
- Impact to perception of the UK government, and scale of intervention to manage damage to reputation.
- Financial impact that would result from regulatory, litigation, citizen redress or other direct costs, including exit costs and break clauses.
- Impact on external stakeholders, including economic loss and/or significant inconvenience.
- Extent of resource hours lost, or additional workload hours required following outage.
- Level of difficulty in improving the system due to significant co-dependency on other systems.