

Good practice guide

Cyber and information security



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 2020, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £926 million.

Contents



Introduction

- Why this issue requires attention 4
- Why audit committees need to monitor cyber risks 5
- What we have found through our work 5
- How government policy has changed in this area 6



Our guidance

- How this guidance links to other standards 7
- What this guidance covers 7
- High-level questions 8
- More detailed areas to explore 10



Further resources 16


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.


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

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



Introduction

- 1** In September 2017, we published the first version of our good practice guide on cyber security and information risk for audit committees.
- 2** Gaining the appropriate assurance for the critical management and control of cyber security and information risk can seem complex. Our aim is to support audit committees to work through the complexity, to understand and question the management of cyber security and information risk.
- 3** Since we published the previous guide, there have been several changes which affect the way in which we interact with and manage our information that can drive increased risk. These include changes to the way we work and live due to the COVID-19 pandemic and the ongoing demand to digitise and move to cloud-based services. The strategic advice, guidance and support provided by government has also been updated to keep pace with these changes, detailing the impact and risks on the management of cyber security and information risk.

Why this issue requires attention

- 4** Information is a critical business asset that is fundamental to the continued delivery and operation of any government service.
- 5** Departments and public bodies must have confidence in the confidentiality, integrity and availability of their data. Any personal data collected, stored and processed by public bodies are also subject to specific legal and regulatory requirements.
- 6** Cyber incidents pose an increasing threat to public bodies' management of their information, with hacking, ransomware, cyber fraud and accidental information losses all evident throughout the public sector. Since our last guide was developed there has been an increasing prevalence of targeted ransomware, including those which can cause serious disruption to an organisation's operations.
- 7** A realistic understanding of cyber issues is essential to protecting public services and their users, particularly as the drive to make public services digital continues. In many organisations, the knowledge and skills available to deal with this issue has not kept pace with the risks.

8 The increase in remote and diverse ways of working, and the move to more cloud-based services, has increased the complexity of management and risk. In addition, complexity arises when public bodies need to share data. Organisations need to have mutual trust in each other's ability to keep data secure and take assurance from each other's risk management and information assurance arrangements for this to happen successfully.

9 Not getting this right can mean that government fails to deliver its core services or gain the benefits of joining up services, and its information is at increased risk (for example, of cyber exploitation or breaching legislation).

Why audit committees need to monitor cyber risks

10 As government's guidance to audit committees makes it clear, cyber security is an area of management activity that audit committees should scrutinise.¹

11 Together with the rapidly changing nature of the risk, this means that there is an important role for audit committees in understanding whether the organisation is adopting a clear approach to cyber, including overall engagement and management. Ensuring compliance with the required rules, standards and legislation, and that there are adequate resources with the required skills and capabilities to carry out these activities is fundamental.

What we have found through our work

12 In September 2016, we published our report on *Protecting information across government*.² The report describes the devolution of the government's approach to cyber and information security and the lack of coherence between the various bodies responsible for governance, oversight and incident response. The establishment of the National Cyber Security Centre (NCSC) in 2017 as a centralised hub has brought together cyber expertise, support, advice and guidance. However, a more recent study carried out across government confirmed that there are still wide differences between departments in terms of the maturity of cyber security assurance available to management.

13 Our 2021 report on *The challenges in implementing digital change* highlights the cyber risks posed by legacy systems, a lack of adequate management and controls, and not transitioning or transforming into modernised systems and services.³

¹ Audit and Risk Assurance Committee handbook (publishing.service.gov.uk). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/512760/PU1934_Audit_committee_handbook.pdf

² Available at: www.nao.org.uk/report/protecting-information-across-government/

³ The challenges in implementing digital change – National Audit Office (NAO) Report. Available at: www.nao.org.uk/report/the-challenges-in-implementing-digital-change/

14 In separate pieces of work on digital skills and online fraud, we have also noted the considerable challenge the public sector has in recruiting and retaining staff with the right experience, and the lack of coordination across government and law enforcement agencies in dealing with criminal cyber activity.

How government policy has changed in this area

15 In the past much of the guidance, governance, mandatory standards and compliance regimes were provided by the centre of government. In 2016 government published a *Cyber security strategy 2016–2021*, with the aim of protecting both the UK economy and the privacy of citizens. As a part of this strategy the NCSC was set up, with the aim of providing a hub of expertise for business and individuals.

16 One of the roles of NCSC has been to bring together the multiple standards and areas of guidance which exist, and to operate as a single point of contact. These include 10 Steps to Cyber Security, ISO 27001, ISO/IEC 27002, the National Institute of Science & Technology (NIST) Cyber Security Framework, Cyber Assessment Framework, Cyber Essentials, Get Safe Online and Cyber Aware. While the NCSC provides support for some of these frameworks and standards, it is still down to individual departments and bodies to define, develop and deliver their approach to cyber risk, ensuring this is appropriate to the organisation's overall operating model and risk appetite.

17 While this approach gives individual organisations the freedom to make decisions, it also means that it is their responsibility to make their own assessments of what standards or frameworks they wish to adopt, and how they are to be assessed and assured.



Our guidance

How this guidance links to other standards

18 This guidance sets out to supplement existing standards and government guidance, and not to replace or re-write it. The sections below have been developed using both government guidance on cyber security and our knowledge through working across our client base, with a view to supporting how audit committees address both the strategic and critical operational issues, while ensuring that the overall context of the issue is clear, and that the questions which are presented also represent key areas of focus.

What this guidance covers

19 What we mean by cyber security is the activity required to protect an organisation's data, devices, networks and software from unintended or unauthorised access, change or destruction via the internet or other communications systems or technologies. Effective cyber security relies on people and management of processes as well as technical controls.

20 Cyber security is part of the wider activity of information security. Information security is a broad term that encompasses electronic, physical and behavioural threats to an organisation's systems and data, covering people and processes. Increasingly, it also plays a part in supporting organisational resilience.

21 In focusing on cyber security, this guidance largely considers the security of electronic data and related processes and transactions. For some organisations with large volumes of paper records who need to secure physical access, wider information security activity can be just as important to safeguard their operational performance or reputation.

High-level questions

22 In engaging with management to explore the maturity of cyber security, audit committees may wish to consider various high-level issues first before discussing points of detail or technical activity. From our experience of auditing the performance of a number of different client bodies, we think the following issues represent a good set of initial topics for discussion.

23 In each case, we have set out a high-level question and some aspects of what a good answer might look like, although these may vary by organisation. Overall, management should be able to describe a balanced approach which considers people (culture, behaviours and skills), process, technology and governance to ensure a flexible and resilient information and cyber security response.



Question 1

24 Has the organisation implemented a formal regime or structured approach to cyber security which guides its activities and expenditure?

- There should be an information security management system in place and under active management, covering policy, processes, governance, skills and training.
- This might involve formal certification through schemes such as Cyber Essentials or ISO 27001/ISO IEC 27002. This may have been implemented or certified by consultants or specialist bodies from government.
- Boards, working groups and individuals should have been allocated specific responsibilities for managing cyber risks.
- There should be plans for resilience and recovery in place and these should be tested regularly.
- There should be a clear assessment of the potential risk arising from electronic links with any supply chain or operational partners.



Question 2

25 How has management decided what level of risk it will tolerate and how it will manage that risk?

- The board should have discussed its overall approach, based on a clear and common understanding of the range of information assets it holds and agreed which of those are critical to the business.
- There should be a clear understanding of the kind of threats and risks the organisation actually faces, based on incident reporting and relevant performance indicators.
- The organisation proactively manages cyber risks as an integrated facet of broader risk management, including scrutiny of security policies, technical activity, information security breach reporting, user education and testing and monitoring regimes.
- The organisation may be involved in sector or peer information exchange mechanisms to improve its understanding.



Question 3

26 Does the organisation understand if its risk profile and appetite has changed due to COVID-19?

- There should be evidence of how working practices have changed as a result of COVID-19; these should be documented and presented as changes to operating models and workforce planning and clearly set out the cyber security and information risk presented, including mitigations and plans.
- In some cases, to meet the demands placed on an organisation due to COVID-19, changes to process, working practices and policy were made quickly. It is important that there is evidence that a review of the required re-development and realignment, including assurance on cyber security and information risk, has been carried out.
- It is important to understand if staff have been provided with adequate cyber security and information risk training and support, both throughout changes to workforce planning and operating models, and in an environment of stabilisation and new ways of working. Organisations need to understand the overall change process they have experienced, including the overall impact on risk, and set out how a current and future business-as-usual workforce plan and operating model will take cyber security and information risk into account.



Question 4

27 Has the organisation identified and deployed the capability it needs in this area?

- There is either sufficient staff capability to deal with cyber security issues or formal arrangements made to secure this capability from external providers.
- There may be actively managed plans in place for the recruitment and retention of staff with specialist security skills.
- There should be clear policies on the handling and storage of data, based on relevant legal requirements, such as the Data Protection Act 2018.
- There is training available for all staff to ensure appropriate levels of awareness and compliance.
- Testing may be conducted to measure the effectiveness of controls.

More detailed areas to explore

28 The NCSC has set out a cyber security toolkit for boards and has identified 10 steps for cyber security to help organisations manage cyber risks. Based on these we have set out below a series of more detailed questions that audit committees may wish to ask management in order to gain assurance that effective controls are in place.

29 As part of its assessment, audit committees should consider the quality of the evidence underpinning the assurances provided by management, including whether there is good evidence that the policies and procedures are well designed, consistently implemented, and operating effectively with an appropriate compliance regime, in all relevant areas of the business.



30 Risk management

- Is cyber risk management part of the overall strategic and delivery planning of the organisation?
- As part of its strategic and operational planning, does the organisation have a clear understanding of its critical services, associated risk appetite and required overall approach to resilience, including cyber?
- Is there a cyber and information risk strategy, detailing overall service landscapes, including shared responsibility models such as cloud, planning and mitigation?
- Are there appropriate cyber and information risk frameworks, management and controls in place?
- Are the governance arrangements for managing cyber and information risk based on the importance of data and criticality of services?
- Do information professionals liaise with central government, stakeholders and suppliers to understand the threat?
- Does senior management understand and engage with risk mitigation processes and promote a risk management culture?



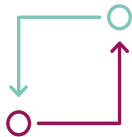
31 Engagement and training

- Is there a clear centralised cyber security training and engagement plan?
- Does the organisation offer cyber specialist training and career routes?
- Is there a clear understanding of skill and capability gaps?
- Does the organisation have security policies covering acceptable and secure use of data?
- Are there grade and role appropriate levels of staff training covering secure processes and use of systems?
- Are there appropriate controls in place to cover the increase in remote and mobile working?
- Are staff aware of information security and cyber risks?
- Do staff know how to report issues and incidents?



32 **Asset management**

- Does the organisation define and utilise asset management systems?
- Is there an asset management register detailing associated risks and linked to cyber security activities?
- Is there a clear understanding of critical and prioritised services, detailing associated cyber and information risks?
- Does the organisation understand the risks associated with legacy asset management?
- Is there a future plan for managing asset management cyber and information security risks?



33 **Architecture and configuration**

- Does the organisation have a business, data and technology architecture, where associated cyber and information risks are mapped and understood?
- Does the architectural landscape include service providers and suppliers, systems and services, with mapped cyber and information risks?
- When planning and deciding on new services is there clear guidance on how cyber and information security should be assessed?
- Are there effective monitoring, backup and recovery systems in place?



34 **Vulnerability management**

- Is there a clear understanding of vulnerability management and process, and its associated risks?
- Are vulnerability management and asset management linked to gain a landscape view of cyber and information risks?
- Are potential high-risk legacy assets identified and managed? If necessary is there a plan in place to address legacy remediation?
- Are there effective vulnerability controls in place, such as automation/manual scanning, monitoring, patches and updates?
- Are vulnerabilities tested on a regular basis, using methods such as penetration testing or red team exercises?



35 Identity and access management

- Are there appropriate identity and access management policies, including passwords?
- Are there effective account management processes, with limits on privileged accounts?
- When using cloud technologies is there effective management of service accounts?
- Are user privileges controlled and monitored on the basis of policies for user authentication and access?
- Is access to activity and audit logs controlled? Are these logs reviewed for unusual behaviour?



36 Data security

- Is the organisation's data architecture and data model detailing levels of security defined?
- Does the data architecture include where partner services are used such as for cloud?
- Does the required legal compliance for data form part of policy? Is it understood, managed and implemented effectively?
- Is the required level of data security and compliance understood, managed, assessed and assured?
- Is there a process in place for data monitoring and unusual behaviour detection?
- Are there appropriate backup and resilience processes and policies in place?
- Are there adequately secure device re-use, repair and disposal processes and policies in place?



37 Logging and monitoring

- Does the organisation have an appropriate logging and monitoring system?
- Does the organisation have the necessary skills and capability to interpret the information provided? Where outsourced specialist partners are used are the responsibilities for acting on information clearly defined?
- Are there adequate automated monitoring systems and services in place?
- Do logs and other monitoring activities enable the identification of unusual activity that could indicate an attack?
- Can logs support investigations by showing who accessed what, when they did so and what they did to the information?



38 Incident management

- Are there incident management plans in place and are these tested?
- Does the incident management plan include a response and test plan?
- Are there specific processes and policies to manage both the risk and the mitigation of a ransomware incident?
- Does the organisation have an incident response and disaster recovery capability, with suitably trained staff?
- Are potential criminal incidents reported to law enforcement bodies and relevant data breaches reported to the Information Commissioner's Office within the timescales required by law?



39 Supply chain security

- Are the supply chain and the services provisioned well understood?
- Are cloud services in place or being considered?
- Has the organisation followed recognised guidance, such as the NCSC's cloud security principles, before committing to using cloud services?
- Does the organisation have a strategy for the use of cloud services, based on a clear understanding of personal data privacy and consent implications, as well as in-depth analysis of how cloud services will interface securely with existing services, systems and processes?
- Has the organisation undertaken due diligence on proposed cloud suppliers?
- Is there a process to ensure and assure that cyber security and information risk is built into the design, development and deployment of new systems and services?
- Is there a mechanism in place to build cyber security and information risk into the procurement and commercial process?
- Is there a process for ongoing improvement and development for cyber security and information risk through the lifecycle and management of the contract?



Further resources

Below is a selection of guidance and insights that may be useful.

1 Government guidance

Strategy

National Cyber Security Strategy 2016 to 2021, National Cyber Security Strategy (NCSC), published 1 November 2016, last updated 11 September 2017. Available at: www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Toolkits

Board Toolkit, NCSC, published 21 March 2019.

Available at: www.ncsc.gov.uk/collection/board-toolkit

10 Steps to Cyber Security, NCSC, published 11 May 2021.

Available at: www.ncsc.gov.uk/collection/10-steps

Cloud

Cloud security guidance, NCSC, published 17 November 2018.

Available at: www.ncsc.gov.uk/collection/cloud-security

Security frameworks

NCSC CAF guidance, NCSC, published 30 September 2019.

Available at: [NCSC CAF guidance - NCSC.GOV.UK](http://NCSC.CAF.guidance-NCSC.GOV.UK)

Security maturity

HM Government IA Maturity Model (IAMM), NCSC, Published 8 March 2018, Reviewed 15 November 2018.

Available at: www.ncsc.gov.uk/information/hmg-ia-maturity-model-iamm

2 National Audit Office (NAO) work on information and cyber security

The digital skills gap in government: Survey findings, December 2015. Available at: www.nao.org.uk/report/the-digital-skills-gap-in-government-survey-findings/

Protecting Information across government, September 2016.

Available at: www.nao.org.uk/report/protecting-information-across-government/

Online fraud, June 2017. Available at: www.nao.org.uk/report/online-fraud/

The challenges in implementing digital change, July 2021. Available at: www.nao.org.uk/report/the-challenges-in-implementing-digital-change/

© National Audit Office 2021

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

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

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



National Audit Office