National Audit Office

Good practice guide

Cyber and information security

Cyber security and information risk guidance for Audit Committees

SEPTEMBER 2017

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of £734 million in 2016.

Contents

1 Introduction 4

2 Our guidance 6

3 High-level questions 7

4 More detailed areas to explore 9

5 Additional questions 12

6 Further resources 14

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

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

1 Introduction

Our interactions with audit committees across the public sector suggest that, alongside rising awareness of the risks associated with cyber security, there is still considerable uncertainty about how committees can best exercise their responsibilities in this area. We have therefore produced this guidance to help them consider the issues involved and structure their discussions with management representatives.

Why this issue requires attention

Information is a critical business asset that is fundamental to the continued delivery and operation of any government service. 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.

Cyber incidents pose an increasing threat to public bodies' management of their information, with hacking, ransomware, cyber fraud and accidental information losses all present throughout the public sector. A realistic understanding of cyber issues is essential to protecting public services and users, particularly as the drive to making public services digital continues. In many organisations, the capability of staff to deal with this issue has not kept pace with the risks.

An additional 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. Not getting this right means that either government fails to deliver the benefits of joining up services or puts its information at increased risk by sharing it across a wider network.

Why audit committees need to monitor cyber risks

As government's guidance to audit committees makes clear, cyber security is now an area of management activity that audit committees should scrutinise.[1] Together with the rapidly changing nature of the risk, this means that there is an important role for audit committees in understanding whether management is adopting a clear approach, if they are complying with their own rules and standards and whether they are adequately resourced to carry out these activities.

1 www.gov.uk/government/uploads/system/uploads/attachment_data/file/512760/PU1934_Audit_committee_handbook.pdf

What we have found through our work

In September 2016, we published our report on *Protecting information across government*.[2] The report describes this 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.

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.

Through our financial audits we routinely find weaknesses in financial system controls. We conducted detailed system audits on 30 bodies in 2017, of which 24 had access control weaknesses. We also frequently find issues in system change controls, business continuity, and third party oversight.

How government policy has changed in this area

In the past much of the guidance, governance, mandatory standards and compliance regimes were provided by the centre of government. The 2014 Government Security Policy framework remains the primary reference point for central government in this area.[3] But the centre of government is increasingly stepping away from prescribing how individual departments and bodies should approach cyber risk, believing that each organisation's operating model and risk appetite should drive its own, separate response.

While this approach gives individual organisations 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. Government has issued various sets of standards or guidance, from *10 Steps to Cyber Security*, to *Cyber Essentials*, *Get Safe Online* and *Cyber Aware*, but has not always made clear who should use which of these. In addition, bodies in some sectors, such as defence, have developed specific approaches which they use with suppliers. Others are using industry standards such as ISO 27001.

The newly established National Cyber Security Centre is bringing together some guidance and advice, but it often relates to a specific area such as the use of passwords or principles for cloud security, rather than providing an overall framework. All of this means it is vital for public bodies to decide what overall framework or approach is most suitable for them.

2 www.nao.org.uk/report/protecting-information-across-government/
3 www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

2 Our guidance

How this guidance links to other standards

We do not wish to add to the problem described above by producing yet another set of guidance. The guidance set out in Part 4 is therefore based on the government's *10 Steps to cyber security*. We have however supplemented it in two ways. Firstly, in this section, we have considered some over-arching questions that may help audit committees address strategic issues before getting into areas of detail. Secondly, in Part 5, we have listed some other challenges not covered by the *10 Steps* guidance, to cover newer or emerging areas of technology.

What this guidance covers

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

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. Data can of course be stored both electronically and physically (e.g. on paper).

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 or which need to secure physical access, however, wider information security activity can be just as important to safeguard their operational performance or reputation.

3 High-level questions

In engaging with management to explore the issue 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.

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.

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

a There should be some kind of information security management system in place and under active management, covering policy, processes, governance, skills and training.

b This might involve formal certification through schemes such as Cyber Essentials or ISO 27001. This may have been implemented or certified by consultants or specialist bodies from government.

c Boards, working groups and individuals should have been allocated specific responsibilities for managing cyber risks.

d There should be plans for resilience and recovery in place and these should be exercised regularly.

e There should be a clear assessment of the potential risk arising from electronic links with any supply chain or operational partners.

2 How has management decided what risk it will tolerate and how does it manage that risk?

a The board should have discussed its overall approach, based on a clear and common understanding of the range of information assets it holds and agreeing which of those are critical to the business.

b 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.

c 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.

d The organisation may be involved in sector or peer information exchange mechanisms to improve its understanding.

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

a There is either sufficient staff capability to deal with cyber security issues or formal arrangements made to secure this capability from external providers.

b There may be actively managed plans in place for the recruitment and retention of staff with specialist security skills.

c There should be clear policies on the handling and storage of data, based on relevant legal requirements, such as the General Data Protection Regulation.

d There is training available for all staff to ensure appropriate levels of awareness and compliance.

e Testing may be conducted to measure the effectiveness of controls.

4 More detailed areas to explore

The National Cyber Security Centre has identified 10 steps for cyber security to help organisations manage cyber risks. Based on these 10 steps 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.

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.

1 Information risk management regime

- Are the governance arrangements for managing information risk based on the importance of data?
- 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?

2 Secure configuration

- Does a system inventory exist?
- Are security patches applied regularly?
- Are vulnerability scans conducted regularly?
- Is there a minimum defined security requirement included in the baseline build for all devices?
- Have higher risk device users (e.g. non-executive board members, temporary staff) been identified and managed?

3 Network security

- Is the network perimeter managed?
- Do information professionals identify, group and protect critical business systems?
- Are security controls monitored and tested?

4 Managing user privileges

- Are there effective account management processes, with limits on privileged 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?

5 User education and awareness

- 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 staff aware of information security and cyber risks?
- Do staff know how to report issues and incidents?

6 Incident management

- Does the organisation have an incident response and disaster recovery capability, with suitably trained staff?
- Are there incident management plans and are these tested?
- Are potential criminal incidents reported to law enforcement bodies and relevant data breaches reported to the Information Commissioner's Office?

7 Malware protection

- Are there effective anti-malware defences in place across all business areas?
- Is there regular scanning for malware?
- Are there controls to filter access from web browsers?
- What changes have been made as a result of monitoring results?

8 Monitoring

- Is there a monitoring strategy in place for all ICT systems and networks?
- 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?

9 Removable media controls

- Is there a policy on the use of removable media (e.g. flash drives)?
- Is data encrypted before storage on removable media?
- Are media scanned for malware before being linked to the system?

10 Home and mobile working

- Is there a clear policy on mobile working, with associated training?
- Is a secure baseline build applied to all mobile devices?
- Are data protected outside formal work environments, including in transit?

5 Additional questions

Because technology has developed since the 10 Steps guidance was published and continues to evolve, we have added below some additional questions on two critical areas which are increasingly having an impact on organisations' cyber security postures: using cloud services and developing new technology or services.

1 Using cloud services

- Has the organisation followed recognised guidance, such as the National Cyber Security Centre'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? This might include assessing:
    - their security accreditation and protocols;
    - contract liability for data losses or service unavailability;
    - whether they have a reputable in-house security team;
    - their approach to proactive testing and historical evidence of how they have responded to security issues;
    - whether the organisation is allowed to perform its own security testing; and
    - the organisation's ability to retain control of information when leaving the cloud provider.
- Has the technical architecture of the system, or the supplier's system, been reviewed by an appropriate security expert, providing an independent assessment of the system's design to ascertain whether the system provides a reasonable level of mitigation for potential attacks?
- Where cloud services are already being used, does the organisation have processes for checking performance against agreed security practices?
- Are plans to mitigate data loss in place, for example using point-in-time backups?

2 Development of new services or technology

- Have security considerations been formally assessed as part of new product or service development?
- Have decision-makers understood security and risk trade-offs through business cases and investment decision processes?
- How far has the organisation relied on others' research versus its own to understand the security of the new technology?
- Are system development activities undertaken in a separate environment from live services?
- How has the proposed network been designed to ensure control and, if necessary, separation of devices from other parts of the organisation's network?

6 Further resources

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

Government guidance

1 2014 Government Security Framework:

www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

2 Cloud guidance:

www.ncsc.gov.uk/guidance/how-confident-can-you-be-cloud-security

www.ncsc.gov.uk/guidance/cloud-security-standards-and-definitions

3 Security frameworks:

www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks

www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

4 Assessment of organisations information security maturity – previously centrally mandated but still used by many departments:

www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm

www.ncsc.gov.uk/content/files/guidance_files/GPG40%20-%20Information%20Assurance%20Maturity%20Model%20-%20issue%202.1%20Oct%202015%20-%20NCSC%20Web.pdf

NAO work on information and cyber security

1 The digital skills gap in government: Survey findings

www.nao.org.uk/report/the-digital-skills-gap-in-government-survey-findings/

2 Protecting Information across government

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

3 Online fraud

www.nao.org.uk/report/online-fraud/

National Audit Office

Design and Production by NAO External Relations
DP Ref: 11613-001