Appendix 2

Cyber security and information risk guidance for Audit Committees

National Audit Office – Good practice guide.

3. High Level Questions

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

There is no organisation wide Cyber Security Strategy, but IT are developing a Cyber Security investment roadmap, informed by multiple external audits and reports, to improve this area.

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

There is no formal Information Security Management System (ISMS) in place. NCC has many components of an ISMS, such as Security Policies, procedures and technical controls, but these are not drawn together in an ISMS framework. A formal ISMS, such as ISO 27001, requires a significant investment of resources, and buy in across the business; it is not an IT function but a business management process.

For background, the following excerpts from itgovernance.co.uk explain what an ISMS looks like:

A. A centrally managed framework for keeping an organisation's information safe
B. A set of policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of information.
C. Includes not only technical controls but also controls to treat additional, more common risks related to people, resources, assets and processes.
D. Based on a risk assessment across the organisation that considers internal and external risks. This means all risks are assessed, analysed and evaluated against a set of predetermined criteria before risk treatments (controls) are applied. Controls are applied based on the likelihood and potential impact of the risks.
E. A framework that helps you make appropriate decisions about the risks that are specific to your business environment.
F. Dependent on support and involvement from the entire business – not just the IT department – from the cleaner right up to the CEO.
G. Not an IT function but a business management process.

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.*

NCC are Cyber Essentials certified. ISO 27001 takes a more comprehensive approach, focussed on organisational risk management.

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

ICT Services has a risk management process, IT Security Team and Security Architect, and the business has a Data Protection Officer, Information Governance Team, Information Governance Group and G&E committee.

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

The organisation completes business continuity exercises, and ICT has a Major Incident process which is tested frequently.

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

Supply Chain risks are mitigated as part of the ongoing supplier and third party management processes which have recently been strengthened as part of the work done by NCC to ensure it is GDPR compliant. All contracts also require suppliers to be Cyber Essentials certified.

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

There is no formal statement of NCC's risk appetite.

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.*

Cyber Security risks have typically been assessed and prioritised within ICT Services rather than at board level.

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.*

Cyber Security KPIs are collated within ICT Services.

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.*

Cyber risks are managed within ICT Services rather than part of broader organisational risk management but security policies, information security breach reporting and user education are managed organisation wide.

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

The IT Security Team are part of the NCSC Cyber Security Information Sharing Partnership (CiSP) and chair the East Midlands Group Warning Advice Reporting Point (EMGWARP).

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.

Cyber security threats are increasing, and so must the technical and procedural controls required to protect NCC from them. ICT Services are looking at ways to automate more cyber security threat prevention to reduce the pressure on the limited resources.

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

ICT Services utilises cyber security contractors to fill any skills gaps.

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.

A completely updated set of IT Security policies covering the handling and storage of data have been written and are due to be published in December.

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

Cyber security training is provided to all staff, with supplemental training provided to staff who handle particularly sensitive data, such as Social Care staff.

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

Staff are tested on their understanding as part of their cyber security training. Other controls are audited as part of NCC's Cyber Essentials, IG Toolkit/DSP Toolkit and PSN compliance.

4. More detailed areas to explore

1. Information risk management regime

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

Increasingly, the classification data affects the way the information risk is handled, throughout IT and IG security standards and related controls.

- *Do information professionals liaise with central government, stakeholders and suppliers to understand the threat?*

ICT Services work with the National Cyber Security Centre (NCSC and CiSP), as well as though external consultancy, to understand the threats.

- *Does senior management understand and engage with risk mitigation processes and promote a risk management culture?*

Cyber Security risk management is conducted by ICT Services. Information risks are managed by the Information Governance Team. There is no overarching or dedicated Cyber Security Risk Management process or group.

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?*

ICT Services use Microsoft's System Center Configuration Manager (SCCM) to provide a system inventory in conjunction with a Patching Standard to direct patching frequency. ICT Services are working towards running regular vulnerability scans to supplement the annual vulnerability scans conducted as part of compliance regimes. All builds are based on National Cyber Security Centre best practice and devices are configured to mitigate security risks regardless of the user.

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

Next Generation firewalls are used to manage the network perimeter. Currently, all systems are protected equally, and key security controls are 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?*

Account management processes exist that limit and monitor the assignment of privileged accounts and policies exist that cover the assignment of other user privileges. Log monitoring is not routinely undertaken, but ICT Services are investigating funding opportunities from the Local Government Association cyber security stocktake to supplement the logging and monitoring capability.

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?

Security policies cover the acceptable and secure use of data. Specific application training is provided to staff for some systems or with particular roles, and all staff receive general cyber security training which includes who to report issues to.

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?*

An IT Security Incident Response Standard ensures that key third parties are informed, such as the Police or ICO, and a IT Major Incident Process covers disaster recovery. Cyber Security Incident Response processes for common incidents are fully documented and tested. The Security Incident Response Standard details who to report incidents to, including the Police and the ICO.

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?*

Sophos anti-virus provides real time protection to all devices combined with firewalls configured to detect and prevent malware at the network level and to filter malicious content from the internet. Full activity logs are kept to investigate any issues.

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?*

A Protective Monitoring Standard ensures that logs can be monitored to detect attacks and for subsequent forensic analysis. Log analysis is currently manual and therefore quite limited. ICT Services are investigating funding opportunities from the Local Government Association cyber security stocktake to supplement the logging and monitoring capability

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?*

The use of removable media is included as part of the Anti-malware and Encryption Standards, ensuring that removeable media data is always encrypted and scanned for malware.

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?*

The Remote Access Standard provides the mobile working policy. NCC uses a VPN solution for remote working, providing protection for data in transit that is securely built into all devices requiring no user intervention and therefore no training to be able to use it securely. A baseline build from the National Cyber Security Centre is used for all mobile devices which includes full disk encryption, protecting data at rest.

5. *Additional questions*

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?*

NCC has used the NCSC's cloud security principles to guide the use of cloud services. A cloud first strategy is underpinned by a Cloud Security Standard and related procedures and processes, such as the DPIA process, that ensure the security of information is maintained within the cloud.

All cloud service providers are comprehensively assessed before being utilised, in proportion to the information classification being stored or processed. Where OFFICIAL-SENSITIVE information is involved, external security accreditation and penetration testing is used as part of the assessment.

Cloud service providers are not periodically rechecked for performance against agreed security practices.

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?*

Security controls are assessed for all internal system developments, including vulnerability scans and external independent penetration testing where the data classification and risk require it, as described by the System Configuration and Management Standard. New systems, especially those with a specific cyber security purpose or risk, are assessed by referring to external testing reports, such as those provided by Gartner or the NCSC.

System development is separated from live at a functional level whilst firewall segmented networks ensure network access is only provided where required.