Nottinghamshire County Council

Report to Governance and Ethics Committee
21 July 2020

Agenda Item: 11

REPORT OF THE SERVICE DIRECTOR FOR FINANCE, INFRASTRUCTURE AND IMPROVEMENT

UPDATE ON THE NATIONAL AUDIT OFFICE CYBER SECURITY AND INFORMATION RISK GUIDANCE FOR AUDIT COMMITTEES

Purpose of the Report

1. To provide Members with an update to the report reviewing the advice for audit committees on cyber security provided by the national audit office (NAO).

Information and Advice

Background

2. A report was presented to the Governance and Ethics committee in July 2019 which briefed Members on the advice published by the NAO for audit committees on the subject of cyber security.

3. The report included an assessment of the current position of the authority against the questions posed by the advice. Members of the Governance and Ethics committee agreed to receive an update to the report in 6 months' time.

Current state assessment

4. The guidance groups the questions into three sections:

    a. Section 3. High level questions
    b. Section 4. More detailed areas to explore
    c. Section 5. Additional questions

3. High Level Questions	Dec 18	June 19	Dec 19	June 20
1. Has the organisation implemented a formal regime or structured approach to cyber security which guides its activities and expenditure?	Amber	Amber	Amber	Green
2. How has management decided what risk it will tolerate and how does it manage that risk?	Red	Amber	Green	Green
3. Has the organisation identified and deployed the capability it needs in this area?	Amber	Amber	Amber	Green

Assessment summary:

5. Question 3.1 is now rated as green from amber. A formal IT Security Strategy is now produced annually, incorporating compliance and best practice. This guides activities and expenditure in cyber security. IT Security policies are reviewed annually and NCC's cyber security is externally certified against Cyber Essentials, the Public Services Network Code of Connection and the Data Security Protection Toolkit.

6. Question 3.2 continues to be rated green. The governance arrangements for information risk deliver a more corporate approach to information risk management through the information governance management board.

7. Question 3.3 is now rated as green from amber. Both the ICT Security and Information Governance Teams are appropriately resourced and trained. There are clear policies covering IT security and data protection, supplemented with appropriate staff training. Significant investments in new technology are being implemented currently, better protecting endpoint devices and servers, improving email filtering and extending cyber security defences to align with the move to cloud-based Office 365 services.

4. More detailed areas to explore	Dec 18	June 19	Dec 19	June 20
1. Information risk management regime	Amber	Amber	Amber	Green
2. Secure configuration	Green	Green	Green	Green
3. Network Security	Green	Green	Green	Green
4. Managing User Privileges	Amber	Amber	Amber	Green
5. User education and awareness	Green	Green	Green	Green
6. Incident management	Green	Green	Green	Green
7. Malware protection	Green	Green	Green	Green
8. Monitoring	Amber	Amber	Green	Green
9. Removable media controls	Green	Green	Green	Green
10. Home and mobile working	Green	Green	Green	Green

Assessment summary:

8. Question 4.1 is now rated as green from amber. The classification of data is a key driver for risk management activities, including the Data Protection Impact Assessment (DPIA) procedure. NCC's information professionals liaise with central government, stakeholders

and suppliers as necessary, and there is engagement in risk management across the authority involving senior management where appropriate.

9. Question 4.4 is now rated as green from amber. Additional procedural controls in ICT coupled with new Microsoft tools limit the use of privileged accounts and provide additional monitoring and oversight. New investments in protective monitoring platforms for 2020 provide active monitoring of activity and audit logs to help detect unusual behaviour. These are supplemented by system level process controls tied to the DPIA procedure that ensure all systems storing or processing NCC data have their access controls appropriately managed.

5. Additional questions	Dec 18	June 19	Dec 19	June 20
1. Using Cloud Services	Green	Green	Green	Green
2. Development of new services or technology	Green	Green	Green	Green

Summary

10. Improvements have been targeted at areas previously rated as amber, ensuring that all controls are now to be rated as green. This demonstrates a strong organisational and technical position with respect to cyber security.

Other Options Considered

11. None.

Reason for Recommendations

12. As all control measures are now assessed as green, Members are asked to agree that the Council is now compliant.

Statutory and Policy Implications

13. This report has been compiled after consideration of implications in respect of finance, equal opportunities, human resources, crime and disorder, human rights, the safeguarding of children, sustainability and the environment and those using the service and where such implications are material they are described below. Appropriate consultation has been undertaken and advice sought on these issues as required.

RECOMMENDATIONS

That the Committee:-

1) Agrees that the Council can now be assessed as compliant with the National Audit Office's cyber security requirements.

2) Considers whether any further actions or information are required on this issue.

Nigel Stevenson
Service Director Finance, Infrastructure and Improvement

For any enquiries about this report please contact:
Mark Davies, Head of ICT (Interim)

Constitutional Comments (KK 01/07/2020)

The recommendations fall within the remit of the Governance and Ethics Committee by virtue of its terms of reference.

Financial Comments: (SES 30/06/2020)

There are no specific financial implications arising directly from this report.

Background Papers

None

Electoral Division(s) and Member(s) Affected

All