Nottinghamshire County Council

Report to Governance and Ethics Committee
24th July 2019

Agenda Item: 6

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 of 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 on 18th December 2018 which briefed Members on the advice published by the NAO for audit committees about 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 4. Additional questions

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

Assessment summary:

5. Question 3.1 continues to be rated as amber. Progress has been made in this area with the production of an ICT security strategy which provides the blueprint for the development of a formal information security management system (ISMS). This security strategy forms part of a structured approach to activities and investment in cyber security which improves our assessment of the current state. However, this does not yet warrant a green status. The introduction of an ISMS involves many interdependent components of technical capability and process change. At a time of significant technical change in the guise of the migration to the cloud and the replacement of our wide area network, careful consideration needs to be undertaken of these interdependencies and their impact on other programmes of work. This is ongoing and is estimated to require a further 12 months before completion.

6. Question 3.2 is now rated as amber from red. Recommendations considered and implemented by Information Governance Group to strengthen the governance of information risk have significantly reduced the concerns raised in the original report. The new governance arrangements deliver a more corporate approach to information risk management. Progress towards a green status will be made via recommendations to be submitted to this new governance board over the next 6 months.

7. Question 3.3 continues to be rated as amber. Pilots of the tools that automate some of the threat prevention capability are underway and will result in relevant business case(s) being produced. Recommendations resulting from these pilots will be made to the ICT management team in the 3rd quarter of 2019/20 for consideration and recommendations to be made to the information governance board.

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

Assessment summary:

8. Question 4.1 remains assessed as amber. As stated in the original report, plans are in place to exploit new tools available once migration to the new cloud-based services is complete in 2019 and this will strengthen the position and hence the assessment. These plans include additional risk reduction measures which will be applied specifically to systems handling higher risk data. We are also looking to strengthen our cyber security defences based on threat intelligence from a wider base, including Canadian, American and Australian government security data and open internet security groups.

9. Question 4.4 remains assessed as amber. As we move to the Cloud we are implementing additional authorisation controls for privileged accounts and tightening the integration between IT and HR to ensure that user access rights are appropriate for their current role within the Council and change when their role changes.

10. Question 4.8 continues to be assessed as amber. Protective monitoring is a primary theme of the IT Security Strategy 2019. A number of products are being trialled and a business case for funding being drafted. The DPIA process is also addressing log analysis at the application level, with centralised cloud log analysis being developed for enterprise system logs.

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

Summary

11. Although progress has been made in those areas not previously assessed as green, the overall assessment would still be assessed as amber. This reflects the significant technical change being introduced that must be dovetailed into the design and build of new technical solutions and processes.

12. However, the overall cyber security posture remains strong with plans in place for the next 6 to 12 months that will strengthen the position further.

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.

RECOMMENDATION

It is recommended that:

1) Members agree to receive an update report in 6 months' time and consider what further action they wish to take.

Nigel Stevenson
Service Director Finance, Infrastructure and Improvement

For any enquiries about this report please contact:
Adam Crevald, Group Manager Design (ICT)
(0115 9772839)

Constitutional Comments (KK 02/07/2019)

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

Financial Comments: (RWK 03/07/2019)

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

Background Papers

None

Electoral Division(s) and Member(s) Affected

All