AUDIT COMMITTEE
20 DECEMBER 2017

ITEM NO. .....

CYBER SECURITY AND OPERATIONAL RESILIENCE STATUS REPORT

SUMMARY REPORT

Purpose of the Report

1. To provide an update on the Council's current position in relation to cyber security and operational resilience.

Summary

2. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

3. Ensuring cyber security requires coordinated effort throughout our information systems as the threat landscape is constantly changing. ICT Services have a mature and well embedded information security management system based on best practice ensuring that cyber risks continue to be effectively managed.

4. In addition our operational resilience, in particular our ability to respond quickly to and recover from a disruption to key services, is supported by appropriate business continuity plans and our secondary data centre facilities.

Recommendation

5. It is recommended that the status of cyber security and operational resilience be noted.

Reasons

6. To provide the Audit Committee with a status report on cyber security and operational resilience within the Council.

Paul Wildsmith
Director of Neighbourhood Services and Resources

Peter McCann, Information Security Manager : Extension 156494

Background Papers

S17 Crime and Disorder	There is no specific crime and disorder impact.
Health and Well Being	There is no specific health and well being impact.
Carbon Impact	There is no specific carbon impact.
Diversity	There is no specific diversity impact.
Wards Affected	All wards are affected equally.
Groups Affected	All groups are affected equally.
Budget and Policy Framework	This report does not recommend a change to the Council's budget or policy framework.
Key Decision	This is not a key decision.
Urgent Decision	For the purposes of the 'call-in' procedure this does not represent an urgent matter.
One Darlington: Perfectly Placed	There is no specific relevance to the strategy beyond a reflection on the Council's governance arrangements.
Efficiency	Implementation of effective information governance systems and procedures has a positive impact on efficiency.

Background

7. Cyber security and operational resilience were briefly discussed during the consideration on the Information Governance Programme Progress Report at Audit Committee in September. To gain a more comprehensive picture and better understanding of the Council's current position in this regard a status report was requested to be presented to Audit Committee in December.

Current Position

Information security management

8. The most recognised standard for information security management is *ISO27001:2013 Information technology – Security techniques – Information security management systems - Requirements*. It formally specifies a management system that is intended to bring information security under explicit management control.

9. The standard requires that management

    - systematically examines information security risks, taking account of the threats, vulnerabilities, and impacts
    - designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
    - adopts an overarching management process to ensure that the information security controls continue to meet information security needs on an on-going basis

10. Certification to ISO27001 requires an external assessment by an accredited independent company to confirm that an information security management system is in place and working effectively. This includes an assessment of the effectiveness of information security technical and procedural controls.

11. Maintaining certification involves annual audits together with three-yearly full recertification assessments.

12. ICT Services are certified to ISO27001:2013 and have a mature and effective information security management system in place (appendix 1 shows our management process). Our current certificate is due for renewal in August 2020.

Compliance

Public Services Network (PSN)

13. The PSN is the government's secure network, which helps public sector organisations work together, reduce duplication and share resources. In order to use the PSN the Council must have a valid PSN compliance certificate.

14. Certification is an annual process which involves providing evidence of compliance with a range of information security based requirements and controls. Compliance also requires that the security of our network and the devices attached to them is independently assessed for technical vulnerabilities (network penetration testing) against Cabinet Office requirements by an accredited company.

15. Our current PSN certificate is due for renewal in March 2018.

Payment Card Industry Data Security Standards (PCI DSS)

16. PCI DSS is the worldwide standard that was set up to help organisations process card payments securely and reduce card fraud through enforcing tight controls surrounding the storage, transmission and processing of cardholder information.

17. PCI DSS requires an annual self-assessment of compliance with specified technical and procedural information security based controls, supported by appropriate evidence. In addition to the self-assessment, quarterly independent assessments of the security of our network (network penetration testing) by an accredited company are required. The quarterly assessment reports must be submitted to Worldpay (the assessing authority) together with a remediation plan for any 'high risk' issues identified in the report.

18. Compliance assessments are ongoing and the timely delivery of remedial actions is regularly monitored.

Internal vulnerability assessments

19. In addition to the independent compliance assessments ICT Services run monthly internal network vulnerability assessments, the results of which complement the external assessments and are fed into the information security risk treatment plan.

ICT Resilience and Disaster Recovery (DR)

20. The Council's primary data centre is located in Darlington Town Hall, with a secondary (DR) data centre located at Municipal Buildings in Stockton. The DR data centre has fully operational installations of all software and associated hardware for all core infrastructure components and does not require recovery of these elements in the event of a disruption to the primary data centre. It would be a reasonable expectation that under normal circumstances the core services and applications would be functional within 24 hours of a failover to the DR data centre being initiated.

21. All data in the primary data centre is protected for recovery and retention purposes by backups and replication.

22. Backups are scheduled jobs that copy both data (files, databases etc.) and server operating systems to disk based on agreed criteria that maintain data integrity and provide consistent recovery points. This data is retained in the storage area network (SAN) at the primary data centre to enable day-to-day recovery tasks and additional copies are transferred to the DR data centre each day. With a copy of each server operating system and data available in the DR data centre there is an immediately available recovery environment in the event of a disaster. Should single systems fail it would be reasonable to expect that they would be restored within 2 working hours with a maximum data loss of 30 mins.

23. All data held on the SAN in the primary data centre is replicated at least once per day to the SAN located in the DR data centre. This provides an additional source of recovery to complement the data stored in the backup system. These replicated datastores provide the main data recovery source in the event of a disruption to the primary data centre.

24. Networking infrastructure forms the communications backbone that allows traffic to flow between the various ICT components and also provides security functionality that controls access to resources. Live networking infrastructure is present at the DR data centre and immediately available should it be required in the event of a disruption to the primary data centre.

Business Continuity

25. Our approach to business continuity mirrors the Business Continuity System set out in the standard *ISO22301:2012 Societal security – Business continuity management systems – Requirements*. A business continuity strategy underpins the management system and describes the approach taken to managing business continuity. The Council has assessed its operations using a rigid business impact analysis, which identifies its time critical functions. Business continuity plans are produced for all critical functions categorised as class 1 and class 2. These functions are those which have been assessed as having a Maximum Tolerable Period of Disruption (MTPD) of less than 3 hours (class 1) and between 3 hours and 24 hours (class 2).

26. All business continuity plans follow a similar format and are produced to assist the identified critical functions to recover from a business interruption. The key business interruptions considered include loss of ICT, loss of premises, loss of information and loss of staff. All business continuity plans contain a risk assessment which assesses the control measures in place and improvement actions required should that function suffer from a loss of ICT.

Understanding the threat landscape

27. At the heart of understanding and keeping abreast of cyber threats both locally and nationally is ISNorthEast, a regional information security group which is also the North East Warning, Advice and Reporting Point (WARP).

28. A WARP is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions.

29. As shown in Appendix 2 ISNorthEast has close links with key cyber security focussed specialists from both central government (NCSC) and the police (NERSOU).

30. This is not an arms-length relationship; representatives from NCSC and NERSOU regularly attend ISNorthEast meetings, and ISNorthEast members regularly attend NCSC and NERSOU events. This relationship, together with the collaborative working of the ISNorthEast members ensure that the cyber threat landscape remains current and well understood.

31. The Council is represented on the WARP by the Information Security Manager who is an active member of ISNorthEast.

Audit

32. In addition to the compliance and certification assessments our control environment is regularly assessed by both External and Internal Auditors.

33. A review of the financial control environment is undertaken annually by the Council's external auditor, including an assessment of network security, disaster recovery and business continuity planning, and information security incident management. The external audit undertaken in March 2017 raised no significant issues or concerns.

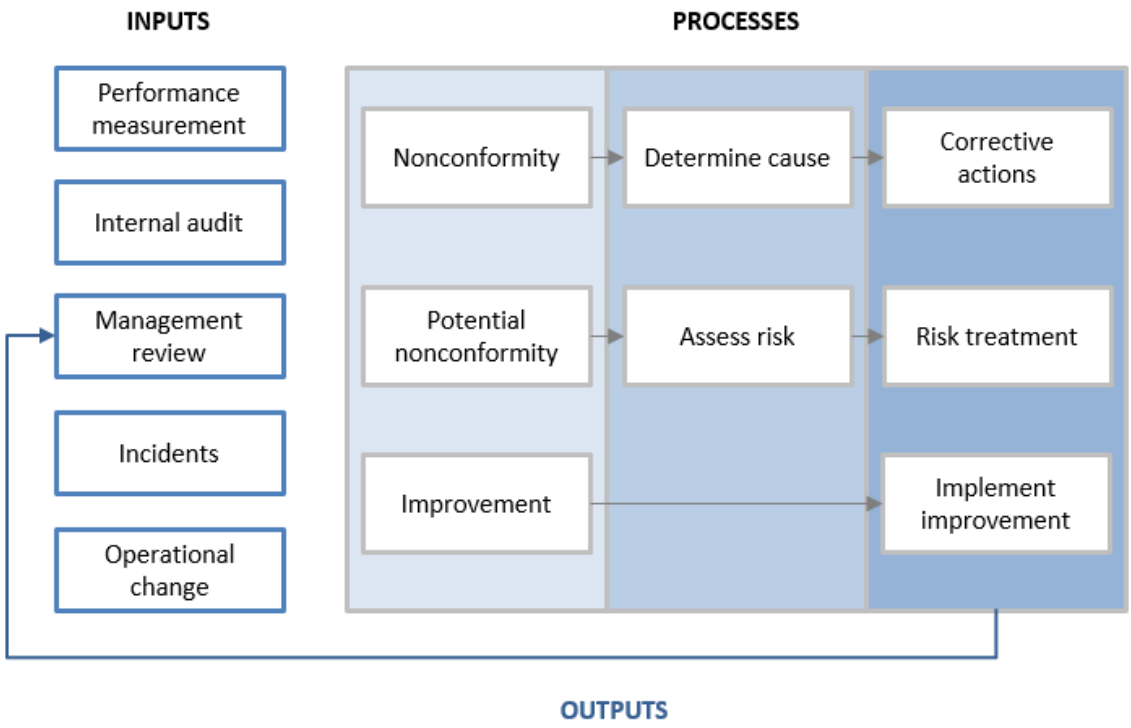
34. The Council's Internal Audit Section has a rolling programme of audits focussing on ICT controls. The programme for 2017/18 covers the following areas:

    - environmental controls (data centre)
    - internet controls
    - email controls
    - backup and disaster recovery

35. The environmental controls audit reported 'full assurance' indicating that, in the opinion of the auditor, a sound system of internal controls is currently being applied which will ensure the system achieves its objectives.

36. The remaining audits in the programme are scheduled but yet to be completed.

Appendix 1 - Information security management process



Appendix 2

National Cyber Security Centre (NCSC)

Set up to protect critical services from cyber attacks, supporting the most critical organisations in the UK, the wider public sector, industry and SMEs.

Cyber Security Information Sharing Partnership (CiSP)

A joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

North East Regional Special Operations Unit (NERSOU)

A collaboration between the three forces of Northumbria, Cleveland and Durham.

Regional Cyber Crime Unit (RCCU)

Dealing with the most serious cyber-dependent offences and providing investigative and technical support and a proactive cyber capability.

ISNORTHEAST

including NEGWARP, the Warning, Advice & Reporting Point for the north east government community

Certificate of Membership

Organisation name **Xentrall ICT Services (Stockton BC & Darlington BC)**

Address Town Hall
Darlington
DL1 5QT

Lead Contact Peter McCann

Valid from 1st April 2017

Expires 31st March 2018

2017-2018

WARP
Warning, advice & reporting point

www.ISNorthEast.org.uk

NORTH EASTERN ICT Partnership
Lead Authority: Gateshead Council, Regent Street, Gateshead NE8 1HH
www.neict.org @NEICT