AUDIT COMMITTEE – 14TH DECEMBER 2016

SUBJECT: IT SECURITY AND GOVERNANCE ACTIVITY UPDATE

REPORT BY: ACTING HEAD OF ICT AND CENTRAL SERVICES

---

1. PURPOSE OF REPORT

1.1 To inform Members of the work carried out by IT Services to assure the security and governance of ICT facilities during the past year.

2. SUMMARY

2.1 Individuals and organisations are increasingly dependent upon IT solutions that underpin their day-to-day work and leisure activities. This increased reliance is accompanied by an escalating risk of systems being either the subject of criminal and malicious attacks or inadvertent mis-use of information.

2.2 IT Services works throughout the year monitoring, maintaining and enhancing the Authority's defences to minimise the risks faced. These activities are independently assessed by external bodies on an annual basis and this report has been compiled to inform Members of the processes involved to certify Caerphilly County Borough Council's approach.

2.3 This report will outline three assessments undertaken during the past year.

- ISO27001:2013 IT Security Standard Accreditation – Outcome of Triennial Audit by BSI
- Public Services Network (PSN) Connection Compliance – Outcome of Annual IT Health Check
- Grant Thornton External Auditor Report – IT General Controls

3. LINKS TO STRATEGY

3.1 Effectively monitoring and managing the Council's IT security and governance measures supports the provision of higher quality and more effective services to the public across all service areas.

3.2 Minimising the risk to IT facilities and the information contained therein contributes to the following Well-Being Goals within the Well-Being of Future Generations Act (Wales) 2016:

- A prosperous Wales – The citizens' financial and personal records are maintained appropriately and securely.
- A resilient Wales – Making Wales a more difficult place to perpetrate cyber-crime safeguarding prosperity and avoiding service interruptions.
- A globally responsible Wales – Setting an example to others that such issues are worthy of the effort involved to minimise the impact of cyber-crime and the highlight the advantages of effective use of information.

4. THE REPORT

4.1 ISO27001:2013 IT Security Standard Accreditation – Outcome of Triennial Audit by BSI.

4.1.1 ISO 27001 is the de facto international standard for information security management that provides a framework to ensure an organisation fulfils its responsibilities that demonstrate a clear commitment to information security management.

4.1.2 The Council has been accredited since 2004 passing each of its annual audits since this date and every third year a more detailed, in-depth assessment is undertaken.

4.1.3 During the summer of 2016, the Council underwent its fourth triennial audit during which time all aspects of its Information Security Management System were scrutinised. The assessment was successfully completed and identified only two minor non-conformities that were resolved before 30th September 2016.

4.1.4 Appendix 1 contains a copy of the Certificate of Registration for the three year period beginning 17th September 2016.

4.2 Public Services Network (PSN) Connection Compliance – Outcome of Annual IT Health Check

4.2.1 The PSN is the UK Government's high-performance secure IT network created to help public sector organisations work together, reduce duplication and share resources.

4.2.2 The services the Council accesses over PSN are:

- The DWP's Customer Information Service used by Housing Benefits and Social Services Finance staff.
- The Youth Offending Service's Libra database.
- The Blue Badge Information Services BBIS used by Customer Services for disabled parking badges.
- The IER (Individual Electoral Registration) system used in Electoral Services.
- GCSX secure email, used by many staff across the Council for sending personal or sensitive data to other public sector organisations.
- Tell Us Once service used by Registrars and other key areas of the Authority.

4.2.3 The PSN demands stringent measures to control access to these shared services. The PSN compliance process exists to provide the PSN community with the confidence that services will work without problems and ensure that their data is protected.

4.2.4 Access to the PSN is allowed only to those organisations that hold a valid PSN compliance certificate. The award of a PSN compliance certificate demonstrates that the Cabinet Office is satisfied that an organisation's security arrangements, policies and controls are sufficiently rigorous to allow you to interact with the PSN and those connected to it.

4.2.5 During the past few months, the Council's IT facilities have been subjected to the PSN Annual IT Health Check. This is a comprehensive assessment that was successfully completed and a compliance certificate was awarded on 18th November 2016.

4.2.6 Appendix 2 contains a copy of the PSN Connection Compliance Certificate for the twelve month period beginning 18th November 2016.

4.3 Grant Thornton External Auditor Report – IT General Controls

4.3.1 During April 2016, the external auditor undertook an IT General Controls Review Audit associated with user management and access controls applied to major systems.

4.3.2 The outcome of the audit was positive with only three resultant observations categorised as “Deficiency - risk of inconsequential misstatement” two of which have been resolved and one is currently the subject of a current management action plan.

5. WELL-BEING OF FUTURE GENERATIONS

5.1 This report contributes to the Well-being Goals as set out in Links to Strategy above. It is consistent with the five ways of working as defined within the sustainable development principle in the Act.

- Long Term – The regular and detailed monitoring and maintenance of IT security and governance standards help to prepare the Council for the challenges of the future.
- Prevention – The measures in place are a proactive response to the increasing risks that will be faced by individuals and organisations in the future. Minimising the likelihood of disruption and making it more difficult for malicious activity to be perpetrated against the organisation is a key foundation from which to move forward.
- Integration – Annually re-affirming the Council’s approach to IT security will safeguard our continued access to PSN and other services as confidence is derived from ISO27001 and PSN compliant status.
- Collaboration – Certified secure IT facilities will facilitate collaboration as consistent, effective measures will be in place to foster inter-organisational working.
- Involvement – Many of the measures that impact on IT security and governance are reliant upon the users of the IT facilities provided. Awareness raising and training are critical to ensure that consumers of IT services are conversant with the principles of effective IT security and governance.

6. EQUALITIES IMPLICATIONS

6.1 This report is for information purposes only, therefore the Council’s full equalities impact assessment process has not been applied.

7. FINANCIAL IMPLICATIONS

7.1 There are no direct financial implications arising from this report.

8. PERSONNEL IMPLICATIONS

8.1 There are no direct personnel implications arising from this report.

9. CONSULTATIONS

9.1 All consultation responses have been reflected in this report.

10. RECOMMENDATIONS

10.1 The Audit Committee is asked to note the content of this report.

11. REASONS FOR THE RECOMMENDATIONS

11.1 To ensure that the Audit Committee is aware of the independent scrutiny of the work undertaken associated with IT security and governance over the past year.

12. STATUTORY POWER

12.1 Local Government Act 2000.

Author: Paul Lewis - Acting Head of ICT and Central Services
Consultees: Gwyn Williams – Acting IT Operations Manager
Alessandra Veronese – Acting IT Development & Support Manager
Stephen Jordan – Principal ICT Security Officer
Wesley Colyer – ICT Security Officer
Joanne Jones – Corporate Information Governance Manager

Appendices:
Appendix 1 ISO/IEC 27001:2013 Information Security Management System Certificate of Registration
Appendix 2 PSN Connection Compliance Certificate

By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Caerphilly County Borough Council
IT Services Department
Tredomen House
Tredomen Park
Ystrad Mynach
Hengoed
CF82 7WF
United Kingdom

Holds Certificate Number: IS 82432

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The Information Security Management System in relation to the provision of IT operations, IT business support and IT development within the Caerphilly County Borough Council in accordance with version 23 of the Statement of Applicability dated 16 November 2015.

For and on behalf of BSI:

Frank Lee, EMEA Compliance & Risk Director

Original Registration Date: 15/07/2004
Latest Revision Date: 31/08/2016

Effective Date: 17/09/2016
Expiry Date: 16/09/2019

...making excellence a habit.™

Certificate No: IS 82432

Location	Registered Activities
Caerphilly County Borough Council IT Services Department Tredomen House Tredomen Park Ystrad Mynach Hengoed CF82 7WF United Kingdom	The Information Security Management System in relation to the provision of IT operations, IT business support and IT development within the Caerphilly County Borough Council in accordance with version 23 of the Statement of Applicability dated 16 November 2015.
Caerphilly County Borough Council Penallta House Tredomen Park Ystrad Mynach Hengoed CF82 7PG United Kingdom	The Information Security Management System in relation to the provision of IT operations, IT business support and IT development within the Caerphilly County Borough Council in accordance with version 23 of the Statement of Applicability dated 16 November 2015.
Caerphilly County Borough Council Enterprise House Tir Y Berth Industrial Estate New Road, Tir Y Berth Hengoed CF82 8AU United Kingdom	The Information Security Management System in relation to the provision of IT operations, IT business support and IT development within the Caerphilly County Borough Council in accordance with version 23 of the Statement of Applicability dated 16 November 2015.

Original Registration Date: 15/07/2004
Effective Date: 17/09/2016
Latest Revision Date: 31/08/2016
Expiry Date: 16/09/2019

Cabinet Office

12 month

PSN connection compliance certificate

This is to certify that

Caerphilly County Borough Council

has had its compliance reviewed and has demonstrated that its infrastructure is sufficiently secure to connect to the PSN during the following period

18 November 2016	18 November 2017
date issued	expiry date

For and on behalf of the Public Services Network

Mark Smith
Head of PSN

This Public Services Network (PSN) connection compliance certificate is issued following completion of the PSN compliance verification process. It shows that your organisation has successfully achieved PSN compliance by demonstrating to the PSN team that your infrastructure is sufficiently secure that your connection to the PSN would not present an unacceptable risk to the security of the network. Your certificate is valid until the expiry date shown above. It may be withdrawn at any time in accordance with the PSN Code of Connection (CoCo) if it is found that you no longer meet the agreed standards.