RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

MUNICIPAL YEAR 2018/19

AUDIT COMMITTEE **4th February 2019**	**AGENDA ITEM NO. 4**
REPORT OF THE GROUP DIRECTOR, CORPORATE & FRONTLINE SERVICES	**Public Services Network (PSN)**

Author: Louise Evans, Data Protection & Improvement Officer

1. PURPOSE OF THE REPORT

The purpose of this report is to:

1.1 Provide Audit Committee with an overview of the PSN accreditation process along with the outcome from the most recent inspection.

2. RECOMMENDATIONS

It is recommended that Members:

2.1 Acknowledge the PSN accreditation process.

2.2 Acknowledge that the Council successfully achieved its annual PSN re-accreditation in October 2018.

2.3 Receive assurance from the accreditation in respect of the integrity of the Councils ICT infrastructure and systems.

3. REASONS FOR RECOMMENDATIONS

3.1 To assist Audit Committee in discharging its responsibilities in respect of overseeing the Council's overall control environment, and receiving assurance from external inspections undertaken.

4. AUDIT COMMITTEE'S TERMS OF REFERENCE

4.1 The Audit Committee's Terms of Reference states its overall purpose, as follows:

The purpose of the Audit Committee is to monitor the adequacy of the risk management framework and the associated control environment; provide independent scrutiny of the authority's financial and non-financial performance to the extent that it affects the Authority's exposure to risk and weakens the control environment; and to oversee the financial reporting process.

4.2 Section E of the Committee's Terms of Reference goes on to identify the following responsibility in respect of the Council's Risk Management arrangements:

Review, scrutinise and issue reports and recommendations on the appropriateness of the Authority's risk management, internal control and corporate governance arrangements, and providing the opportunity for direct discussion with the auditor(s) on these

5. BACKGROUND

5.1 The Public Service Network (PSN) is a national framework set out by the Government, and managed by the Cabinet Office PSN & Cyber Compliance Team.

5.2 The purpose of the PSN is to unify the network infrastructure across the public sector into an interconnected ''network or networks'' that enables public sector organisations to securely access, collaborate and share services.

5.3 Connection to the PSN network is only permitted subject to the Cabinet Office rigorous annual accreditation process that provides assurance that organisation security and controls meets defined mandatory standards.

5.4 Within Wales we are connected to the PSN via the Public Sector Broadband Aggregations (PSBA). PSBA is a managed network overseen by Welsh Government, which connects public sector organisations in Wales. PSBA enables local health boards, local authorities, Welsh Government, higher and further education, blue light emergency services and other public sector organisations in Wales to securely.

5.5 Further secure connections facilitate integration with a wider range or public services, authorities and agencies in the UK including but not limited to:

- UK Local authorities,
- Central government departments,
- DVLA;

5.6 Specific services access, send and receive data electronically with other PSN connected agencies as part of business process. For example:

- Housing Benefits – to access/use the LA Delivery System (LADS) to securely share information with the DWP.

- Trading Standards – to access/use the Joint Asset Recovery Database (JARD) to record evidence.
- Fraud / Debt Recovery– to access/use the LocTA tracing system in relation to individuals and businesses.

6. ANNUAL PSN ACCREDITATION PROCESS

6.1. Any organisation that has a business need to communicate directly with individual government departments through the PSN network, needs to achieve appropriate accreditation from the Cabinet Office.

6.2. PSN accreditation and compliance is an ongoing annual process that demonstrates to the Cabinet Office and all connected organisations that an organisation appropriate security arrangements, policies and controls in place.

6.3. The Cabinet Office sets out a series of technical, policy and procedural standards that each organisation must meet in order to achieve accreditation. These standards are regularly reviewed and updated by the Cabinet Office in conjunction with the UK governments National Technical Authority for Information Assurance (CESG) that advises organisations on how to protect information and information systems.

6.4. The following highlights the main requirements of the accreditation process:

Information Assurance (IA) Requirements

6.5. The PSN Code of Connection (CoCo) sets out the Information Assurance (IA) requirements that the Council must meet and the commitments it must make to connect and stay connected to the PSN.

6.6. The IA requirements are listed in full in Appendix I of this report and cover areas such as operational security, patch management, physical security, authentication and access controls etc.

Network Schematic

6.7. The council is required to provide an up-to-date documentation of its network infrastructure. This enables the Cabinet Office to understand the infrastructure that the council wants to connect to the PSN and what risks it might present to other users and the network.

Information Technology Health Check (ITHC)

6.8. Public sector bodies that want to connect to the PSN must provide assurance that their networks meet the latest supporting guidelines by undertaking an IT Health Check. (ITHC)

6.9. The ITHC must be undertaken by a government approved external provider that employs penetration testing personnel qualified to assess IT systems for HMG and other public sector bodies.

6.10. The ITHC is essentially an 'audit' required to inform PSN compliance. As part of the ITHC government certified personnel attempt to ''hack'' the Council's network and exploit any weakness that may potentially exist. There are two elements:

i. **External** - Provides assurance that the organisation's external systems e.g. websites, are protected from unauthorised access or change, and they do not provide an unauthorised entry point into systems.

ii. **Internal -** Internal systems are tested to provide further assurance that no significant weaknesses with regard to the infrastructure or individual systems that could allow intentionally or unintentionally impact on the security of another.

6.11. Following the audit an 'ITHC PSN CoCo (Internal/External) Security Report' is presented to the council. The report highlights any potential risks or vulnerabilities identified as part of the ITHC and makes key recommendations to mitigate such risks.

6.12. Following receipt of the report the Council is required to create a Remediation Action Plan (RAP) to address and mitigate any risks identified and progress any recommendations. Day-to-day progress against the RAP is monitored by the Data Protection & Improvement Officer as outlined in 5.13 (governance and monitoring) below.

7. GOVERNANCE & MONITORING

7.1 The PSN Annual Re-Accreditation programme of work is managed by the Councils Data Protection Officer and overseen by the Head of ICT. Regular updates on progress is reported to the Information Management Board (IMB) chaired by the Director of Corporate and Frontline Services, designated as the Councils Senior Information Risk Owner (SIRO). The IMB meets bimonthly with any risks, escalations or exceptions provided to the Senior Leadership Team where appropriate.

7.2 Operationally the ICT Service has fortnightly Information Security Group meetings chaired by the Data Protection Officer. The group is made up of representative specialist technology, information and security officers. Whilst the forum drives our PSN requirement, ensuring ongoing integrity is not only an annual requirement in isolation. Work continues throughout the year to proactively review, identify and implement measures to ensure that our systems, networks and infrastructure are safe, secure and up-to-date with the latest possible security technologies.

7.3 The Council is a member of the Warning, Advice and Reporting Point (WARP) and Society of Information Technology Management (SOCITM) Cymru that all 22 Local Authorities in Wales participate, collaborating to share good practice and information on cyber threats, incidents and solutions.

8. PSN RE-ACCREDITATION OCTOBER 2018

8.1 In relation to the Councils 2018 PSN re-accreditation process, the ITHC was commissioned and undertaken by an accredited third party in advance of the October submission date.

8.2 The findings of the ITHC PSN CoCo Internal/External Security Report identified recommendations, the themes of which are as follows:

- Passwords - further strengthen passwords for certain areas.
- Patch Management – apply the latest patches to identified devices.
- Software Updates - deploy the latest software versions to identified devices.
- Device configuration - update configuration settings to secure any potential vulnerabilities.

8.3 On the 26th September 2018 the Councils submission inclusive of the Remedial Action Plan was submitted to the Cabinet Office PSN & Cyber Compliance Team for validation and review.

8.4 On the 22nd October 2018 Council received confirmation that the application had **passed assessment** that the Council meets the requirements of connecting to the PSN. A copy of the Compliance Certificate is included in Appendix II.

9. EQUALITY AND DIVERSITY IMPLICATIONS

9.1 There are no equality and diversity implications as a result of the recommendations set out in the report.

10. CONSULTATION

10.1 There are no consultation implications as a result of the recommendations set out in the report.

11. FINANCIAL IMPLICATION(S)

11.1 There are no financial implications as a result of the recommendations set out in the report.

12. LEGAL IMPLICATIONS *OR* LEGISLATION CONSIDERED

12.1 There are no financial implications as a result of the recommendations set out in the report.

13. LINKS TO CORPORATE AND NATIONAL PRIORITIES AND THE WELL-BEING OF FUTURE GENERATIONS ACT

THE COUNCIL'S CORPORATE PLAN PRIORITIES

13.1. The Council's continued PSN accreditation supports its ability to work directly with, for example, the DWP when delivering services to its citizens.

WELL-BEING OF FUTURE GENERATIONS ACT

13.2. The Well-being of Future Generations (Wales) Act 2015 identifies a core set of activities that are common to the corporate governance of public bodies where change needs to happen. Collaboration is one of the identified core activities. The Council's ability to work collaboratively with the DWP, via the PSN helps to ensure more timely and accurate payments for housing benefits.

14. CONCLUSION

14.1 The Council is required to go through the PSN Accreditation process each year, and this exercise involves a rigorous technical audit of its I.T infrastructure. Following the most recent inspection, the Council's accreditation continued.

14.2 As noted in paragraph 14.1, the PSN audit involves a rigorous technical audit of the I.T infrastructure. From this audit, and in accordance with its Terms of Reference, Audit Committee can receive assurance in respect of the Council's I.T internal control environment.

LOCAL GOVERNMENT ACT 1972

AS AMENDED BY

THE LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

AUDIT COMMITTEE

4th February 2019

PUBLIC SERVICES NETWORK (PSN)

REPORT OF THE GROUP DIRECTOR, CORPORATE & FRONTLINE SERVICES
Author: Louise Evans (Data Protection & Improvement Officer)

Item: 4

Background Papers

None.

Other Information:

Relevant Scrutiny Committee - None.

Contact Officer – Louise Evans

Appendix I

PSN Code of connection Security Requirements:

1. Operational security

We require you to have policies, processes and procedures in place ensuring the secure operation of your infrastructure.

a. Vulnerability management (patch management)

- Even well-managed systems develop vulnerabilities over time. A sensible security policy will not only assess vulnerabilities arising from new systems, hardware etc. but will monitor your existing infrastructure for the emergence of exploitable vulnerabilities. Most vulnerabilities can be fixed by patching (a targeted, specific upgrade to a certain device, application or system). This should be done at regular intervals, dependent on the severity of the vulnerability.
- Where your infrastructure suffers from a vulnerability that you know is being exploited elsewhere (in someone else’s infrastructure, for example) you should apply a patch immediately.
- Not every vulnerability has a patch available, so you need to take some other steps to reduce the potential impact of an exploit against that particular vulnerability.

b. Secure configuration

- The default, out-of-the-box configuration of many of the systems, software and services you use are likely to leave your infrastructure vulnerable. It is important that you have control over the configuration of these elements of your infrastructure and use that control to configure them to provide an appropriate level of security.
- Malicious software (such as viruses or spyware) is one of the most common threats faced by networked infrastructure, so it is important that you have measures in place to protect your infrastructure against these threats. As an absolute minimum you should have good, well-configured antivirus software for all devices, systems and services.
- In order to ensure that secure configuration is achieved across your infrastructure, you need to be able to direct the security patch management for all managed devices.

c. Physical security

- Technical security measures may be futile if the physical environment in which your data is held and processed, and in which your staff work, is not appropriately secured as well. Ensuring that only the right people have access to, or sight of, areas where sensitive assets are stored, held or processed needs a combination of physical measures (such as security guards, access controlled doors, identity cards) and policies and procedures which govern their use, monitor compliance and enable enforcement action.

d. Protective monitoring and intrusion detection

- Any infrastructure should expect to suffer attacks, either targeted or opportunistic. If the infrastructure has connections to the internet this is all but guaranteed. A good protective monitoring policy will help you identify security incidents quickly and provide you with information that will help you initiate your incident response policy as early as possible. It will also help you prevent identical or similar incidents in the future.
- Along with technical controls, you will have businesses processes and policies that promote and ensure the security of your infrastructure. Abuses of these processes pose a significant risk to the security of your organisation, and the security of the PSN.
- We have not provided details of specific information your protective monitoring policy should detect and retain. You should design your policy based on the specific details of your infrastructure and the threats you expect to face.

e. Security incident response

- A crucial aspect of your overall security state is how you respond to incidents when they occur. Your incident response policy should:
  - allow you to mitigate harm quickly and effectively
  - include reporting it to the PSN team and other relevant entities of the situation where appropriate
  - allow you to prevent similar incidents occurring in the future
- Your policy should require you to inform the National Cyber Security Centre (NCSC) of any cyber security incident that it has expressed an interest in, and also keep us informed if the incident impacts the PSN. NCSC reduces the cyber security risk to the UK by improving its cyber security and cyber resilience. It works together with public sector organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. It publishes practical and proportionate security guidance to help protect both new and existing IT systems.

2. Authentication and access control

Sensible authentication and access control ensures your devices and services are safe against unauthorised access but that your users enjoy access to the devices and services that they need. When End User Devices (EUDs) access corporate services, you can provide an appropriate level of security by requiring:

- user-to-device authentication
- device-to-service authentication
- user-to-service authentication

NCSC’s password guidance recommends not relying on password length or complexity to ensure security. Instead, you should look to apply simple technical controls such as locking users out after a specified number of failed authentication attempts or applying two-factor authentication.

3. Boundary protection and interfaces

The boundaries between your network/services and the internet or any other network are the most likely point for an attempted intrusion, so we require you to impose appropriate security controls at these points. A firewall with appropriately configured rule sets

We recognise that you may present services outside of these protected boundaries. In these cases we have imposed additional requirements on how these services communicate with your core infrastructure. We also recognise that BYOD is an increasingly popular strategy for organisations to let their staff work more flexibly, so we have imposed certain restrictions on how unmanaged devices are used in the context of PSN that allow BYOD policies to be used while ensuring they do not present excess risk to the PSN.

4. Protecting data at rest and in transit

You need to make sure that data is protected by default, whether at rest within your infrastructure, in transit within your infrastructure or in transit between your infrastructure and another environment. There are a lot of different solutions that would accomplish these goals. It is up to you to decide exactly how you achieve data at rest and data in transit protection.

5. User and administrator separation of data

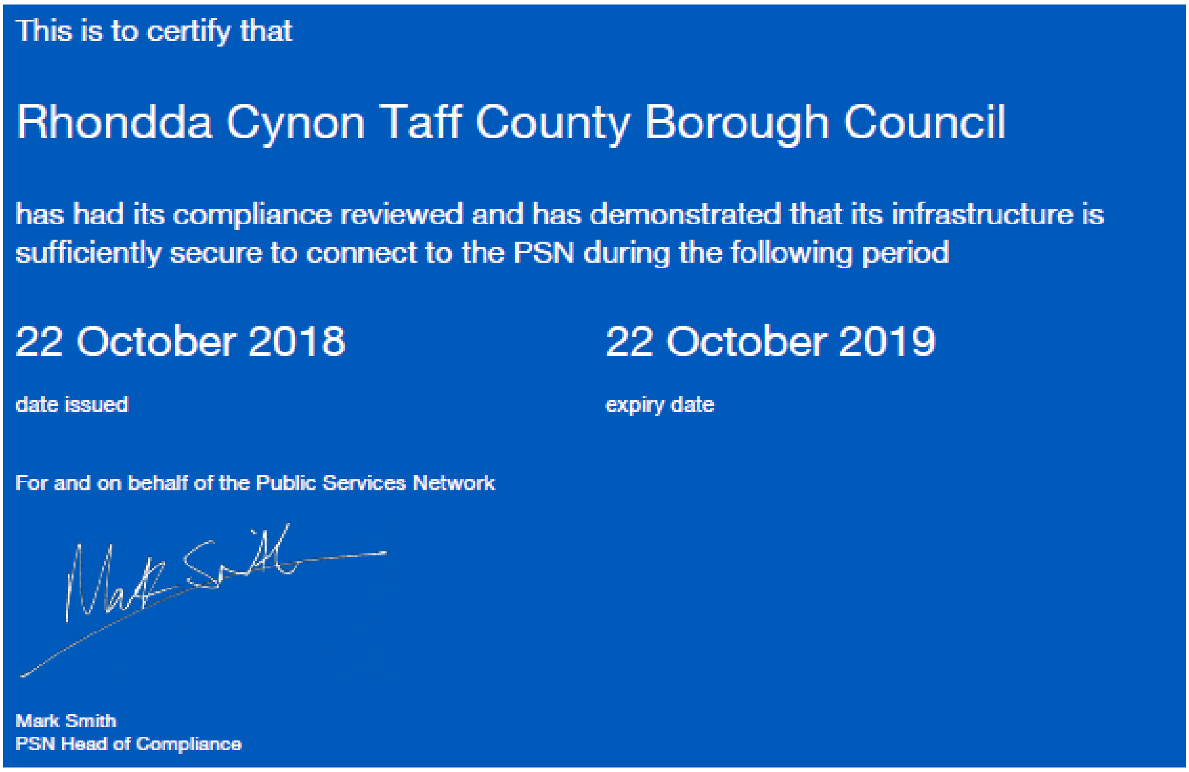
Separation between users prevents one compromised or malicious user posing a risk to others’ data or experience of a service. In general, user access should be based on the principle of least privilege, so that each user should have the minimum level of access necessary to allow them to carry out their function. This principle is true for cloud services and non-cloud services alike.

6. Users

Implementing security controls on your staff helps protect you against the risk of malicious actors inside your infrastructure. The Baseline Personnel Security Standard (BPSS) provides a strong baseline against which to hold those members of your staff who have privileged access to, for example, corporate services or network configuration.

Appendix II

PSN connection compliance certificate



This is to certify that

Rhondda Cynon Taff 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

22 October 2018	22 October 2019
date issued	expiry date

For and on behalf of the Public Services Network

Mark Smith
PSN Head of Compliance

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.