Kirklees
COUNCIL

Report title: Cyber Security Assurance

Meeting	**Corporate Governance and Audit Committee**
Date	**21 February 2025**
Cabinet Member (if applicable)	**Cllr Tyler Hawkins**
Key Decision **Eligible for Call In**	**Yes**

Purpose of Report

- To provide assurance to Corporate Governance and Audit Committee of the council's existing cyber controls and process in line with UK Government standards.
- To update the committee on the work being undertaken to adopt the National Cyber Security Centre's Cyber Assessment Framework, which the LGA and MHCLG are recommending for adoption across the public sector.

Recommendations

- The Corporate Governance and Audit Committee notes the cyber security technical controls and process already in place which meet UK Government expectations.

Reasons for Recommendations

- The council carries out rigorous annual testing and external assessment to achieve Public Sector Network accreditation, which will continue.
- For further assurance, the council has started the process to adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) which will be independently assessed during 2025.
- The council's DSPT submission strictly follows NHS England's (NHSE) guidance for 'Standards Met' but the controls have not been directly audited.

Resource Implication:

- Work to comply with the NCSC's Cyber Assessment Framework will be resourced from within existing teams and become a business as usual process within the IT service.
- The initial work to implement the CAF will be more labour intensive and the MHCLG awarded the council a £15k grant following our first submission to support with any additional cost.

Date signed off by Executive Director & name	Rachel Spencer-Henshall
Is it also signed off by the Service Director for Finance?	Kevin Mulvaney
Is it also signed off by the Service Director for Legal and Commissioning (Monitoring Officer)?	Samantha Lawton

Electoral wards affected:	All
Ward councillors consulted:	None
Public or private:	Public
Has GDPR been considered?	Yes. GDPR requires that personal data must be processed securely using appropriate technical and organisational measures, all of which are covered by the Cyber Assessment Framework.

1. Executive Summary

1.1 Kirklees Council consumes services from the Department for Work and Pensions (DWP) and NHS, amongst others, over private connections through the Public Sector Network (PSN) and Health and Social Care Network (HSCN)

1.2 The council carries out an independent assessment process to connect to the PSN and a self-assessment to connect to the HSCN on an annual basis.

1.3 The National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF) to provide cyber assurance for organisations that provide Critical National Infrastructure (CNI) or deliver Network and Information Services (NIS)

1.4 The Local Government Association (LGA), The Ministry of Housing, communities and Local Government (MHCLG) and Department for Health and Social Care (DHSC) has recommended the adoption of the CAF to bring consistency for cyber assessments across the public sector.

1.5 Kirklees Council have started to work on the adoption of the CAF to ensure our systems and processes meet the standards set.

2. Information required to take a decision

2.1 Kirklees Council and all other local authorities have been consuming central government services, particularly the DWP for benefits data, for 20 years over the Public Sector Network (PSN) The PSN is a ‘walled garden’ network which keeps data private ‘at rest’ and ‘in transit’. Kirklees Council is also connected to the Health and Social Care Network (HSCN) to connect to NHS resources using a similar ‘walled garden’ approach.

2.2 Connections to both networks are checked through two annual processes. PSN accreditation largely tests cyber security controls to ensure connected organisations are not a risk to the network or the data within it. The Data Security and Protection Toolkit (DSPT) accepts the PSN accreditation for its technical controls and extends further into organisational controls to ensure patient data is secure.

2.3 The Council’s last PSN accreditation certificate was awarded on 6 June 2024 following an IT Health Check (ITHC) carried out by an independent assessor in October 2023. The IT Security Team created a remediation plan in November 2023 and the plan was completed to a satisfactory level by May 2024.

2.4 The Council, as a provider of social care, carries out a self-assessment for the NHS Data Security and Protection (DSP) Toolkit 2023 which allows us to measure our performance against the National Data Guardian’s (NDG) 10 data security standards.

2.5 The council’s last DSPT submission to NHS England was on 28 June 2024 and we achieved ‘Standards Met’ which means we do meet the required assurance levels set.

2.6 The toolkit requires an auditor to provide assurance that the mandatory requirements of the self-assessment and that the detail submitted and evidence available substantiates the requirements set out in the Toolkit. This is reviewed annually by Internal Audit.

2.7 The National Cyber Security Centre (NCSC) developed and published the Cyber Assessment Framework in 2018, to provide a cyber assurance framework for organisations that provide Critical National Infrastructure (CNI) or deliver Network and Information Services (NIS)

2.8 Cabinet Office published the “Government Cyber Security Strategy: 2022 to 2030” in February 2022 and the Department of Health and Social Care published the “Cyber Security Strategy to 2030” in March 2023.

2.9 Both national strategies recommended the adoption of the CAF.

2.10 The CAF has four objectives:

- **Managing Security Risk:** This first objective ensures that organisations have the structures, processes, and resources to effectively manage security risks. This involves evaluating the risks to critical services and applying security measures that are appropriate to the threat level.
- **Protecting Against Cyber Attacks:** The second objective focuses on safeguarding systems and services. It ensures that organisations put the necessary technical and procedural safeguards in place to defend against cyber attacks. This includes things like access control, protective monitoring, and secure configuration.
- **Detecting Cyber Security Events:** The third objective covers the detection capabilities that allow organisations to identify potential cyber security incidents. This includes ensuring that systems are in place to monitor and detect any attempts at breaching security.
- **Minimising the Impact of Cyber Security Incidents:** The final objective focuses on resilience and recovery, ensuring that organisations are capable of responding effectively to incidents, maintaining essential services, and recovering quickly after a disruption.

2.11 Local Government CAF submissions will be independently assessed and assured by the The Ministry of Housing, Communities and Local Government (MHCLG). There are currently no plans to replace the PSN accreditation process with the CAF so it will be a further assurance process.

2.12 The council will need to carry out a DSPT submission to NHSE by June 2025. Whilst the NHS are moving to CAF this year, it is unknown as to when NHSE will instruct councils to follow suit and switch from completing an annual DSPT to accepting a CAF.

2.13 The timeline for implementing the CAF is as follows:

- Get CAF Ready (completed October 2024)

  We identified and assessed three critical business systems. Those systems were SAP, Revenues and Benefits and Adult Social Care.

- Organisational Assessment (target April 2025)

  Objectives to be assessed: Managing Security Risk and Minimising the impact of cyber security incidents. We are in the process of providing responses to the assessment criteria in the CAF. The evidence produced will be submitted in early February and will be reviewed and assessed by an independent assurer from the MHCLG. An improvement plan will be created following the assessment and submitted to MHCLG.

- Assessment of Critical Systems (planned May – September 2025)
  Objectives to be assessed: Protecting against Cyber Attacks and Detecting Cyber Security Events. We will assess the controls and processes in place to protect our three critical systems. Two of the systems are in public cloud environments and one on premise. On completion of this stage, there will be a need to repeat this process for all other systems in the council over a longer period.

2.14 The aim is to meet the controls in the CAF over a period that is acceptable to both risk management and assurance requirements and continuous improvement.

2.15 Officers will report back to the Information Governance Board on a quarterly basis to update on project progress, issues found and any emerging risks.

2.16 Officers will update provide updates on the adoption of the CAF to Executive Leadership Team twice a year, Portfolio Holder twice a year and Overview and Scrutiny Management Committee on an annual basis.

3. Implications for the Council

3.1 Council Plan

The implementation of the CAF has no impact on the delivery of the council plan, but failure to meet the requirements of the CAF could result in damaging impact in the event of a cyber attack. Previous cyber attacks in other local government organisations have resulted in significant impact lasting years with financial impact of up to 20% of the overall revenue budget of the council.

3.2 Financial Implications

The council received a grant of £15k from the MHCLG on completion of the “Get CAF Ready” stage in the national project. The work to complete the CAF will be largely officer time within the IT Service and absorbed within existing workloads.

3.3 Legal Implications

The council must continue to improve its cyber security posture, resilience, responsiveness and recovery from cyber attacks using the CAF and by adopting the national and regional strategies to ‘Defend as One’. Failure to do so will result in incalculable financial loss and significantly impact residents

3.4 Other (e.g. Risk, Integrated Impact Assessment or Human Resources)

- **Risk**

  Cyber security is a tier one threat to national security and is treated as such within the council. The council consumes services that span multiple government agencies and undertakes the necessary steps to protect data when at rest and in transit.

- **Integrated Impact Assessment (IIA)**

  The cyber assurance processes have no impact.

4 Consultation

Not applicable.

5 Engagement

The IT Service regularly engages with organisations across the region with the Yorkshire and Humber WARP (Warning Advice & Reporting Point) and the MHCLG on the implementation of the CAF and the continued PSN accreditation.
The Head of IT is also the regional lead on behalf of the Integrated Care Board for the

development of a West Yorkshire Cyber Strategy that delivers against the Department of Health & Social Care's national strategy.

6 Options

Not applicable.

7 Next steps and timelines

The IT Service will continue the work of adopting the CAF and provide an update to Corporate Governance and Audit Committee in 12 months.

8 Contact officer

Terence Hudson – Head of Technology

9 Background Papers and History of Decisions

Not applicable.

10 Appendices

More can be read online about the Cyber Assessment Framework here: https://www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-digital-and-technology-policy-team/cyber-assessment

11 Service Director responsible

Andy Simcox – Service Director for Strategy and Innovation