Teignbridge District Council

Audit Committee

2 September 2025

Part 2

CYBER ASSESSMENT FRAMEWORK

Purpose of Report

To present findings from an independent assessment of the Council's cyber security maturity against the Local Government Cyber Assessment Framework (LG CAF).

Recommendation(s)

The Audit Committee is recommended to note the report and use the findings as a source of assurance.

Financial Implications

None. Funding was secured from MCHLG for the three Councils. Costs of ongoing improvement measures are considered to be 'business as usual' and subsequently included in Strata and the Councils' routine budget costs.

Legal Implications

None. Effective cyber security is essential for good governance. The CAF Assessment is expected to become mandatory for Councils in the future. An early assessment is a positive step to help prepare for future compliance.

Risk Assessment

This exercise provides valuable assurance on the extent to which cyber risk is managed and mitigated.

Environmental / Climate Change Implications

None.

Report Author

Sue Heath – Audit & Information Governance Manager
Tel: 01626 215258
Email: sue.heath@teignbridge.gov.uk

Executive Member

Councillor John Parrot – Executive Member for Corporate Resources

1. INTRODUCTION / BACKGROUND

1.1 Cyber security is essential for all internet-connected organisations. In January 2022, the Cabinet Office launched the Government Cyber Security Strategy, which requires public sector bodies to comply with the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF).

1.2 For local authorities, a tailored version of the CAF, known as the Local Government CAF (LG CAF), has been developed, by MHCLG(DLUHC). Councils are assessed against this sector-specific framework to ensure they meet appropriate cyber security standards.

1.3 Arculus, part of Bridewell (a security company used by MHCLG), has played a key role in developing the LG CAF and now conducts independent assessments on behalf of MHCLG. In December 2024, the Council successfully completed the CAFReady entry stage, securing funding and an independent review of CAF Areas A (Managing Security Risk) and D (Minimising the Impact of Cyber Security Incidents), carried out by Arculus.

1.4 Given the shared IT infrastructure across the three councils, Arculus proposed a joint evaluation of common systems and processes before reviewing each Council's individual arrangements. Evidence was provided by all three Councils and presented by the Strata IT team during two dedicated audit sessions.

2. KEY FINDINGS

Area A: Managing Security Risk (Achieved)

Strengths:

- Strong governance at board level.
- Well-documented policies, roles, and communication channels.
- Effective risk management processes.

Area D: Minimising Impact (Not Achieved)

Three medium risks were identified:

- D1.a – Response Plan: Limited supplier engagement in incident response.
- D1.c – Testing & Exercising: Insufficient intelligence-driven testing.
- D2.b – Learning from Incidents: Poor documentation of improvement actions.

Areas of Good Practice

The assessment highlighted:

- **Strong governance:** Clear leadership and cyber security policies.
- **Proactive engagement:** Comprehensive submissions with well-documented evidence.
- **Established processes:** Board-level oversight with strong communication channels.
- ***Assessor informal feedback**:* The assessor praised the Council's submission, noting that the minimal number of risks, which suggested the Council was placed it in the top quartile of organisations assessed and that the overall cyber maturity appeared to exceed MHCLG's level 2 target.

Recommendations

To improve cyber security maturity and meet LG CAGF requirements the following actions are recommended:

- **Incident Response Plan (D1.a):** Strengthen engagement and testing.
- **Testing & Exercising (D1.c):** Conduct comprehensive, intelligence-led tests with clear documentation.
- **Learning from Incidents (D2.b):** Implement structured processes to review, implement and test improvements.
- **Improve evidence collection***:* Later CAF assessments will require clearer evidence of:
  - Cyber communication understanding across roles, with comprehension.
  - End-to-end role clarity from leadership to members and technical teams (e.g., Strata).

Next Steps for the Council

1. Review findings with internal stakeholders.
2. Develop a detailed **Improvement Plan** (timelines, responsibilities, resources).
3. Proceed with Strata's **"Security as a Service" remediation programme:**
   - **Framework Definition:** Detail requirements and effort estimates.
   - **Approvals & Resource Allocation:** Seek Tri-Council Architecture Board approval.
   - **Implementation:** Commit resources, track progress.

Conclusion

The assessment confirms the Council has a strong foundation in cyber security risk management. By addressing the identified gaps, we can enhance our maturity and align with national expectations for local government.