Report for:	Audit Committee
Date of Meeting:	30 September 2025
Subject:	**Cyber & Information Security Update**
Cabinet Member:	Cllr David Wulff, Cabinet Member for Quality of Living, Equalities and Public Health
Responsible Officer:	Lisa Lewis, Head of Digital Transformation & Customer Engagement
Exempt:	N/A
Wards Affected:	N/A
Enclosures:	None

Section 1 – Summary and Recommendation(s)

The following report provides a high-level update on Cyber and Information Security activities over the last 12 months. The report aims to assure the Audit committee of ongoing vigilance and remediation work around Cyber and Information Security risks.

Recommendation(s):

1. **Recommendation – That the committee note the report.**

1.0 Introduction

1.1 The council's ICT and Information Management teams are responsible for ensuring that cyber and information security risks are appropriately mitigated. These operational activities are overseen by the IT and Information Governance (ITIG) board which meets every two months.

1.2 Significant risks and outputs from ITIG are referred to the leadership team for information and further strategic direction.

2.0 Audit Activities

2.1 In 2024 the Ministry of Housing, Communities and Local Government (MHCLG) launched the initial stages of the Cyber Assessment Framework (CAF) for local government.

2.2 Mid Devon District Council (MDDC) took part in a 'Get CAF Ready' project alongside other councils to commence assurance work around our cyber and information security risk management. We successfully completed the project which resulted in a £15k grant to invest in improvements in our cyber posture as an organisation.

2.3 After the 'Get CAF Ready' project, MHCLG offered participating councils the opportunity to obtain independent assurance in this area. This was being offered free of charge and MDDC took that opportunity.

2.4 During the first quarter of 2025 MDDC participated in an external audit with MHCLG's chosen partner Bridewell. The result was a CAF improvement plan identifying areas where further improvements could be made to mitigate risks.

2.5 Devon Audit Partnership (DAP) provided project assurance on the above activities and were an active partner in the process providing invaluable help and guidance during the process.

2.6 In addition to the above DAP is in the process of conducting further internal audits on Firewalls and Patch Management which will be reported to this committee.

3.0 Improvement Projects

3.1 As part of the CAF assurance work it was found MDDC had good governance around cyber and information security, and no further work was required.

3.2 One of our recent activities included a full risk review and assessment. This was supported by the Performance and Risk manager and ratified by ITIG. The findings will be reviewed by Leadership team. Additionally, DAP will be conducting an internal audit on risk management in this area later this year.

3.3 The revised risk register is an operational document that is reviewed every two months by ITIG and/or quarterly as part of the risk management cycle of the council. This may, or may not, affect the corporate risk management score over time. It is a live document and will be updated depending on our ability to mitigate current and emerging threats.

3.4 Other recent activities include:

- The purchase and implementation of a 24/7 managed extended detection and response service for threat detection, monitoring, and incident response services.
- Full roll-out of Multi Factor Authentication (MFA) on end-point devices.
- The recent procurement and current implementation of a system for managing risks around our supply chains for cyber and data.
- Market research on improved cyber and data protection awareness training and phishing simulations.

4.0 Conclusion

Officers and management of the council continue to be vigilant about cyber and information security. The nature of cyber risks means that we will never be able to fully mitigate risks and that those risks will change over time. However, plans exist for continuous monitoring and mitigation as part of the operational management of the council's infrastructure and systems as a priority.

Financial Implications - The report does not have any specific financial implications. Future decisions on investment, e.g. Disaster Recovery provision or resourcing will be made via senior leadership or the ITIG Board as operationally appropriate.

Legal Implications - The report does not have any specific legal implications. Appropriate levels of governance around cyber and data security help to mitigate potential liability or legal action from data loss.

Risk Assessment - This report details activities against the current Corporate Cyber and Information Security risks.

Impact on Climate Change – There are no impacts or opportunities around climate change because of this report.

Equalities Impact Assessment - This report does not have any impact under Equalities.

Relationship to Corporate Plan - ICT and Information Management underpins all corporate activity. It is therefore essential that our cyber and data security practices and protections are robust to ensure business continuity and the delivery of all services.

Section 3 – Statutory Officer sign-off/mandatory checks:

Statutory Officer: Maria de Leiburne
Agreed on behalf of the Monitoring Officer
Date: 16 September 2025

Chief Officer: Stephen Walford
Agreed by or on behalf of the Chief Executive/Corporate Director
Date: 16 September 2025

Performance and risk: Steve Carr
Agreed on behalf of the Corporate Performance & Improvement Manager
Date: 17 September 2025

Cabinet member notified: yes

Report: Exclusion of the press and public from this item of business on the published agenda on the grounds that it involves the likely disclosure of exempt information. No

Appendix: Exclusion of the press and public from this item of business on the published agenda on the grounds that it involves the likely disclosure of exempt information. No

Section 4 - Contact Details and Background Papers

Contact: Head of Digital Transformation & Customer Engagement
Email: llewis@middevon.gov.uk
Telephone: 01884 234981

Background papers: None