Mid Devon
DISTRICT COUNCIL

Report for:	**Audit Committee**
Date of Meeting:	20 August 2024
Subject:	**Cyber Security & Information Governance 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 Security and Information Management activities and risk mitigation over the past few months. It also includes updates on activity and challenges around meeting the high-level audit recommendations as detailed in the Cyber Security and ICT Core Audit 2022 – 23 and the Information Governance Audit 2022 – 23.

Recommendation(s):

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

2. **Recommendation – That the committee authorise an extension of time as detailed below on Cyber Security and ICT Core Audit 2022- 23, item 8.1.**

Section 2 – Report

1.1 At the Audit Committee of 25th June 2024 Devon Audit Partnership (DAP) provided an internal audit annual report 2023/2024. The report provided an update on ICT and Information Management (IM) activities around audit recommendations. The report showed that Cyber Security activity had improved and achieved a status of 'reasonable assurance,' whilst IM had remained at 'limited assurance' and had an increased risk rating of 12.

1.2 The following provides an update on each area and includes a summary of mitigating actions, continuing risk, and challenges around remediation of risk and actions outstanding to comply with audit recommendations.

2.0 Audit Recommendations update - Cyber

2.1 Out of the original 35 management actions, 19 have been completed, 13 being in progress and 3 not yet started. Completed actions include, but are not limited to:

- An IT and Information Governance Board (ITIGB) has been established (alongside appropriate supporting documentation). Cllr David Wulff sits on this board as part of his portfolio.
- A high-level change process document has been created for standard and security system changes.
- An Information Security (cyber / Data Protection) questionnaire is completed as part of the procurement process to gain assurance that a supplier meets the required minimum standards of the Council.
- The completion of cyber training is now averaging between 89-91% over the last two quarters, the variance is in part due to recent increased staff turnover.

2.2 There remains one High outstanding recommendation which ICT have been unable to remediate due to higher priority security work and capacity within the team. The team were reduced by 1.5 FTE within the last twelve months which has impacted our ability to continue improvements. Audit recommendation 8.1 relates to supply chain management and active monitoring or risk impact assessment against software/service suppliers for our main systems/functions. This is a significant administrative burden to complete.

2.3 Focus has been on what we can control and high priority activities. To continue work on audit recommendation 8.1, and further work included below, ICT will be seeking some temporary additional resource to provide some capacity within the team. This is to be partially offset by an Ear Marked Reserve (EMR), and it is the intention to utilise the IM team to help with the administrative burden whilst risk assessments on returns will be completed by the ICT Operations Manager. We are also reliant on suppliers responding promptly and anticipate a significant amount of ‘chasing’ for the information.

It is therefore requested, as per Recommendation 2 above, that the Audit committee authorise an extension of the deadline for this piece of work to March 2025.

2.4 ICT achieved Public Sector Network (PSN) compliance in June 2024.

2.5 Cyber Assessment Framework (CAF) – The Council has, alongside other councils, opted to participate in a Local Digital ‘Get CAF Ready’ project. This was initiated by what was the Department of Levelling Up, Housing & Communities (DLUHC) and is now the Ministry of Housing, Communities & Local Government (MHCLG). The project provides guidance and tools for assessing, documenting, and planning around Cyber governance and response. It follows best practice as set out by the National Centre for Cyber Security (NCSC). Successful completion of this project could result in a small grant which could be used to offset the cost of the additional resources alluded to above.

2.6 As part of their annual ICT audit work, DAP have agreed to provide project assurance of the ‘Get CAF Ready’ project so that resources can be aligned and reduce duplication of effort for all services concerned.

2.7 It is worth noting that the new Government, as part of the recent King’s Speech intend to bring forward a Cyber Security & Resilience Bill. It is too early to know what this will mean for Local Government and cyber security provisions, but progress of this Bill will be monitored by ICT and the ITIG board.

3.0 Information Management

3.1 The last internal audit report placed Information Management at ‘limited assurance.’ Due to the transactional workload of administering Freedom of Information (FOI) and Data Subject Access Requests (DSAR) the team has not been able to make adequate progress on many of the audit recommendations.

3.2 In March 2024 the Data Protection officer (DPO) resigned and the service has been running at 50% capacity.

3.3 Due to the Data Protection and Digital Information Bill that was in progress at the time of the resignation a restructure of the service was initiated. Responsibility for governance and compliance now formally sits with the Head of Digital Transformation & Customer Engagement. A Senior Information Officer replaces the Data Protection Officer (DPO) role. This was recruited to in June 2024 and at the time of this report the Information Management Officer role should have someone in post from 5 August 2024.

3.4 Training for the new roles/recruits will commence immediately and a review of all outstanding audit recommendations and compliance activities with a full programme of work should be ready by early Autumn 2024. This will include the work towards remediation of Cyber Audit recommendation 8.1 as above and a project to improve efficiency of the FOI/DSAR administration with a view to freeing up time for the team to focus on governance, compliance and monitoring work moving forward.

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 Security Risk and addresses currently outstanding High audit recommendations and mitigations required.

Impact on Climate Change - ICT are currently reviewing hardware fleet and software systems with an aim to reduce cost and environmental impact. These will be reported via the Corporate Action Plan updates to Planning, Environment & Sustainability PDG.

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: Andrew Jarrett
Agreed by or on behalf of the Section 151
Date: 8.8.24

Statutory Officer: Maria de Leiburne
Agreed on behalf of the Monitoring Officer
Date: 8.8.24

Chief Officer: Andrew Jarrett

Agreed by or on behalf of the Chief Executive/Corporate Director
Date: 8.8.24

Performance and risk: Steve Carr
Agreed on behalf of the Corporate Performance & Improvement Manager
Date: 01 August 2024

Cabinet member notified: Yes

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