Audit and Governance Committee

Date of meeting:	20 January 2026
Title of Report:	**Cyber Security Risk Response**
Lead Member:	Councillor Kate Taylor (Cabinet Member for Customer Experience, Sport, Leisure and HR and OD)
Lead Strategic Director:	Si Bellamy (Chief Operating Officer)
Author:	Peter Honeywell
Contact Email:	peter.honeywell@plymouth.gov.uk
Your Reference:	Cyber Security Risk Response
Key Decision:	No
Confidentiality:	Part I - Official

Purpose of Report
To provide the Committee with assurance that the Council has responded to the Devon Audit Partnership recommendations for improvement in our arrangements regarding Cyber Security.

Recommendations and Reasons
1. Committee to note the progress made
   Good progress has been made in responding to the audit findings. The Council has continued to prioritise and fund investment in technology and training to provide mitigation against the risk of cyber attack on our systems and data.

Alternative options considered and rejected
1. To not respond to Devon Audit Partnership recommendations for improvement to cyber security arrangements. This would expose the Council to unacceptable levels of risk, the consequences of which could be catastrophic for the organisation. This option is therefore rejected.

Relevance to the Corporate Plan and/or the Plymouth Plan
Delivery of almost all Council services now relies on secure access to our systems and data. A widespread and sustained outage of systems would severely compromise the services we delivered to our residents and our ability to deliver the priorities set out in the Corporate and Plymouth Plans. Cyber security remains one of the top threats faced by the Council.

Implications for the Medium Term Financial Plan and Resource Implications:
Investments required to address the user management automated solution are likely to be funded from a grant anticipated from MHCLG to support us with ongoing cyber security improvements.
The resource implications of the work to manage and mitigate our cyber risks are covered by existing headcount and roles within both Delt and PCC.

Financial Risks

A cyber attack that prevented access to our systems and data for a sustained period of time could potentially have significant financial risk for the Council. Attacks on other Councils have, for example,

prevented them from collecting Council Tax and other income streams. Additionally, other Councils have also struggled to support their residents with services, including financial support services.

Legal Implications

Cyber risk remains one of the Council's highest- scoring threats and engages statutory duties under the UK GDPR and Data Protection Act 2018, including accountability (Article 5(2)), security of processing (Article 32), and breach notification (Articles 33–34). The report demonstrates governance measures such as the updated Cyber Risk Management Policy (OR04), defined roles and responsibilities, a scored risk register, and quarterly incident reporting, but notes that residual risk remains high due to increasing attack sophistication. Audit and Governance Committee are provided with assurance that these controls are effective in mitigating unlawful access risk and confirm that incident response procedures meet statutory notification requirements. Failure to maintain these measures could expose the Council to regulatory enforcement, reputational damage, and potential liability for service disruption or data breaches.

Carbon Footprint (Environmental) Implications:

There are no carbon or other environmental implications resulting from this report.

Other Implications: e.g. Health and Safety, Risk Management, Child Poverty:

** When considering these proposals members have a responsibility to ensure they give due regard to the Council's duty to promote equality of opportunity, eliminate unlawful discrimination and promote good relations between people who share protected characteristics under the Equalities Act and those who do not.*

There are no other implications resulting from this report.

Appendices

**Add rows as required to box below*

Ref.	Title of Appendix	**Exemption Paragraph Number** (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
		1	**2**	**3**	**4**	**5**	**6**	**7**
A	Audit and Governance Cyber Security Report							
B	Recommendation Tracking – PCC Cyber Security – Governance (Risk Management)							
C	Recommendation Tracking – Cyber Governance and Access Management							

Background papers:

**Add rows as required to box below*

Please list all unpublished, background papers relevant to the decision in the table below. Background papers are <u>unpublished</u> works, relied on to a material extent in preparing the report, which disclose facts or matters on which the report or an important part of the work is based.

Title of any background paper(s)	**Exemption Paragraph Number** (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
	1	**2**	**3**	**4**	**5**	**6**	**7**

Information Security Policy – OR04 Cyber Risk Management							

Sign off:

Fin	N/A	Leg	LS/0000360954/LB/13/01/26	Mon Off	N/A	HR	N/A	Assets	N/A	Strat Proc	N/A
Originating Senior Leadership Team member: Si Bellamy											
Please confirm the Strategic Director(s) has agreed the report? Yes Date agreed: 15/01/2026											
Cabinet Member approval: Councillor Taylor approved by email Date approved: 12/01/2026											