Oversight and Governance
Chief Executive's Department
Plymouth City Council
Ballard House
Plymouth PL1 3BJ

Please ask for Hannah Chandler-Whiting
T 01752 668000
E democraticservices@plymouth.gov.uk
www.plymouth.gov.uk
Published 16 January 2026

AUDIT AND GOVERNANCE COMMITTEE – SUPPLEMENT PACK

Tuesday 20 January 2026
2.00 pm
Council House, Plymouth

Members:
Councillor Allen, Chair
Councillor Finn, Vice Chair
Councillors Cuddihee, P.Nicholson, Raynsford and Sproston.
Independent Member Mrs Annette Benny.

Please see additional information relating to agenda items 13 and 14.

Audit and Governance Committee – Supplement Pack

Audit and Governance Committee

PLYMOUTH CITY COUNCIL

Date of meeting:	20 January 2026
Title of Report:	**Armada Way Independent Learning Review – Action Plan Final Report**
Lead Strategic Director:	Tracey Lee (Chief Executive)
Author:	Liz Bryant, Service Director for Legal (Monitoring Officer)
Contact Email:	liz.bryant@plymouth.gov.uk
Your Reference:	
Key Decision:	No
Confidentiality:	Part I - Official

Purpose of Report

To provide the Audit and Governance Committee with a summary of progress made against the implementation and completion of the Armada Way Independent Learning Review (AWILR) Action Plan, following updates presented to the Sub-Committee on 30 October 2025 and 14 January 2026.

Recommendations and Reasons

1. That the Audit and Governance Committee notes:
   - The actions undertaken as required under the AWILR Action Plan have been reported to and monitored by the sub-committee;
   - That the sub-committee have confirmed that they are satisfied with the progress reported and that the requirements of the Action Plan have been met;
   - The sub-committee endorsed the ongoing implementation of longer-term changes, including the full constitutional review and CPMO establishment; and
   - That a full report setting out the recommendations proposed following the review of the Council's approach to the pre-election period is brought the meeting of the Audit and Governance Committee on 10 March 2026.

Reason:
The AWILR review made a number of recommendations for improvement which the Council committed to review and where appropriate implement changes and improvements. The Action Plan requirements have been delivered and the sub-committee was given oversight of the implementation. The A&G Committee is now required to confirm that it is satisfied, based on the recommendations of the sub-committee that the Action Plan has been delivered.

Alternative options considered and rejected

1. To not report the Action Plan progress to the Audit and Governance Committee. This option was rejected as City Council tasked the Audit and Governance Committee, through a specifically constituted sub-committee to monitor the implantation of the Action Plan requirements.

Relevance to the Corporate Plan and/or the Plymouth Plan
The Audit and Governance Committee's oversight of the implementation of the Action Plan supports the Corporate Plan by ensuring that it follows a democratic and co-operative process. The actions undertaken as part of the Action Plan, including the establishment of a CPMO and consultation of the City Centre Mast Plan support the ambitions for growth set out in the Plymouth Plan.

Implications for the Medium Term Financial Plan and Resource Implications:
Additional resources required for CPMO and training; mitigated through planning and existing resource deployment.

Financial Risks

The implementation of the CPMO carries a risk of placing an additional burden on already stretched resources. This will be managed through redeploying existing resources where possible.

Legal Implications

(The completion of the actions set out in the Action Plan ensures the Council's ongoing compliance with governance and legislative requirements. The longer-term implementation of the CPMO and the full Constitutional review will ensure that the Council is not only meeting its legislative requirements but is effectively managing risk and following best practice for implementation of all projects and programmes.

Carbon Footprint (Environmental) Implications:
The implementation of the Action Plan provides enhanced consideration of environmental matters, particularly through the new Tree Management Principles document

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.*
Click here to enter text.

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	Briefing report title							

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 unpublished 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.

<table>
<tr><th rowspan="2"><b>Title of any background paper(s)</b></th><th colspan="7"><b>Exemption Paragraph Number</b> (if applicable)
<i>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.</i></th></tr>
<tr><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Sign off:

Fin	OW.25.26.114	Leg	LS/00003609/54/LB/16/01/26	Mon Off	N/A	HR	N/A	Assets	N/A	Strat Proc	N/A
Originating Senior Leadership Team member: Liz Bryant, Service Director for Legal											
Please confirm the Strategic Director(s) has agreed the report? Yes Date agreed: 16/01/2026											

This page is intentionally left blank

ARMADA WAY INDEPENDENT LEARNING REVIEW

ACTION PLAN IMPLEMENTATION FINAL REPORT

1. Executive Summary:

The Audit and Governance Sub-Committee has overseen delivery of the Armada Way Independent Learning Review Action Plan since October 2025. All actions arising from the review are now complete, with longer-term implementation underway for constitutional review and CPMO establishment. Governance arrangements are legally compliant, project management standards strengthened, and consultation frameworks embedded. Environmental and wellbeing measures have been implemented, and training programmes launched. The Audit and Governance Committee is being asked to note progress and endorse ongoing work to embed improvements.

2. Background

The AWILR report was presented to Full Council on 2 June 2025, accompanied by an Action Plan detailing improvements required. The Audit and Governance Sub-Committee was tasked with monitoring delivery. Initial progress was reported in October 2025, with a final update provided in January 2026 confirming completion of actions arising from the review, subject to longer-term implementation of agreed changes.

3. Summary of actions completed

1. Governance

- External governance review completed; recommendations will be implemented as part of the full constitutional.
- Full constitutional health check underway by external lawyers (approx. 6-month project) which will implemented through oversight provided by the Constitution and Civic sub-committee of Audit and Governance Committee.
- Pre-election Period Guidance reviewed and will be brought to Audit and Governance Committee in March with recommendations for change.
- Governance arrangements now compliant with legal requirements; forthcoming changes will focus on best practice and efficiency.

2. Project Management and Capital Programme

- Proposal for a Corporate Programme Management Office (CPMO) developed to strengthen delivery of complex projects.
- Incremental implementation plan in place; full roll-out by May 2026, subject to resources.
- Capital Programme Handbook comprehensively reviewed and redrafted; updated Terms of Reference for CPOG and Capital Programme Board included.

3. Consultation and Engagement

- New Consultation and Engagement Framework launched internally with supporting resources.

- Recruitment of Engagement and Consultation Advisor ongoing; training plan under development.
- External consultant appointed for City Centre Master Planning consultation.

4. Environmental Regulations

- Tree management principles document drafted, reviewed by Steering Group and Scrutiny Panel; final revisions underway.

5. Employee Wellbeing

- Wellbeing survey completed; results analysed and reported to CMT.
- Procurement of safety devices and wellbeing initiatives underway.
- Recommendations complete but subject to ongoing review.

6. Training and Development Plan

- Governance and project management training developed and rolled out.
- E-learning module for governance training to launch shortly.
- Final governance training session for elected members scheduled.

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 unpublished 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/00 0036 09/54 /LB/1 3/01/ 26	Mon Off	N/A	HR	N/A	Asset s	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											

This page is intentionally left blank

BRIEFING REPORT

Cyber Security Risk Response

1. BACKGROUND

The Council recognises the threat of a major attack on our systems and data to be one of our highest scoring risks on our risk logs. This position is consistent with the national risk assessment, the 2025 National Risk Register - National Risk Register - 2025 edition includes cyber attacks on infrastructure and underlines the importance of protecting our systems and data across critical services supporting our residents.

The National Cyber Security Centre (NCSC) described the threats faced by organisations in the UK in their 2025 annual report - It's time to act - NCSC Annual Review 2025. The threats are varied in nature and origination, but the evidence is clear that significant attacks are increasing and that it requires a management response not just a technical one to effectively counter them.

The systems and data that the Council relies upon to deliver services to our residents were regularly attacked during the last year. The defences we have put in place provide good protection to avoid major issues and we didn't suffer systems unavailability or data theft in 2025. It is however clear that the sophistication of attacks is continuing to rise and as the NCSC describe, organisations should prepare themselves to deal with a successful cyber attack as well as strengthening their defences to help avoid being attacked.

2. RESPONSE

The Council has recognised and accepted the position and responded with the creation of a Cyber and Information Security Board comprising resources from both PCC and Delt with expertise in both the threats we face and how to mitigate them. The Board also includes representation from Devon Audit Partnership in order that they have first-hand understanding of the Council's response to our cyber threat and can contribute their expertise. This board meets monthly and maintains a detailed risk log which is updated regularly to ensure the Council is learning from the experience of others as well as the attacks on our systems.

The board have developed a detailed risk log breaking down the different types of threats the Council faces to our systems and data. The risk log is scored and our highest scoring risks all now have active mitigations in place, including where required investment to support he implementation of the mitigation.

Note: despite the investment and organisation that has gone into the Council's cyber defences over the last 5 years our risk score has broadly stayed consistent. This is because the sophistication of the threat has risen over the same period. Our improved defences have resulted (broadly) in the Council holding our position regarding our exposure to the threat, rather than reduced our likelihood or the impact of an attack.

The board also produce a quarterly report for CMT providing them with details of important cyber incidents occurring in the last 3 months as well as the progress made in mitigating risks.

3. AUDIT FINDINGS

This report provides the Audit and Governance Committee with a response to three specific areas of audit findings that required improvement when they were raised. These are detailed in the spreadsheets used to track the audit recommendations. For clarity the report below summarises the audit findings and the actions taken in response:

Action/audit finding	Response to date	Remaining action
The IT/Cyber Risk Management Policy is overdue for review and has elements that could be strengthened	The Council's Cyber Risk Management policy OR04 has been updated and published on Staffroom ORO4. The detailed recommendations made in the audit finding have been included in the new policy	No further action required
Lack of defined roles and responsibilities for IT Risk Management	OR04 sets out the management roles and responsibilities around cyber security and can be accessed here OR04	No further action required
The known weaknesses in the end-to-end user management processes should be identified at the Cyber Board and the risks appropriately managed. The creation of a risk register to provide transparency and a means of governing the associated risks should be considered. Furthermore, the commencing of a workstream/ project to make the necessary improvements would provide a timeline around which some impetus could be achieved.	The Cyber and Information Governance Board review the Council's risk register on a monthly basis, this register includes risk around user management. The specific risks around account management was mitigated manually whilst the new payroll systems (ITrent) was introduced last year. The Council and Delt are now working on proposals to automate more of this process	Finalise the design and investment requirements for the automated solution to user management. Implement automation using the principle of least privilege (where the minimum permissions and access rights necessary to perform a specific function are provided, and nothing more). Target date: end September 2026

Audit Area	Audit Name	Recommendation Name	Recommendation Description	Status	Priority	Management Action	Update Notes	Target Implementation Date	Please select from the drop down list the current position with implementing this audit recommendation.	Please provide a brief update to support your answer to the previous question, and timescales for implementation. If the recommendation has been implemented please provide the date of implementation.
Resources Directorate (	PCC Cyber Security - Governance (Risk Managemen	The IT/Cyber Risk Management Policy is overdue for review and has elements that could be strengthened	There is a Corporate PCC Risk Management Strategy 2023-2025 in place. The strategy and Organisational Risk Register/System provide the organisational risk management framework. The Corporate Risk Management Strategy does not make specific reference to IT/cyber Risks. This would imply that IT/cyber risks are expected to be managed in line with the corporate strategy. There is also Risk Management Policy (OR04) that specifically relates to IT Risk Management. However there are aspects of Risk Management Policy (OR04) that could be strengthened. For example; Document control refers to a review date of April 2022. It is unclear if this is referring to when it was last reviewed or when it was due for review. Either way the policy would appear to have not been reviewed or updated since April 2022. Lack of detail regarding IT risk management roles and responsibilities. States that risks will be assessed across the organisation (of which there is no evidence, due to no directorate or department Risk Registers or Risks on the Organisational Risk Register regarding IT/cyber risks). It does not state for example who will be responsible for co-ordinating, reporting or maintaining IT/cyber Risk Register. Current owner of the policy is stated as the "Corporate Risk Advisor". This could be more appropriately the Chief Operating Officer (based on Directorate structure and Role Profile i.e. SIRO) or the Assistant Chief Executive (based on Role Profile) or the appropriate service director or the Transformation Architecture Manager (IT Lead Officer - although they may be the owner of many of the risks). Limited reference to the PCC Risk Management Strategy. (only regarding scoring). Provides a link to a risk register template but does not provide link or direction to the Corporate/Organisation Risk Management system. Appear to be written as directed more to service directorates rather than IT itself. A policy of this type should address the roles and responsibilities of both IT and other departments/directorates.	2. Agreed by Management	High	Management accept the observations as set out. Our Risk Management Policy (as part of our Information Security Framework) OR04 would clearly benefit from review. As set out the review of the will address how this policy aligns with our Corporate Risk Management Strategy and processes. OR04 is likely to focus on the specific IT roles and responsibilities, with the intended audience IT and cyber security teams, not business services. Responsible Officer: Information Governance Mgr (JF)	Kirsty Harrison (20 October 202	31/10/2025	FULLY IMPLEMENTED	Implementation was completed in December 2025.
Resources Directorate (	PCC Cyber Security - Governance (Risk Managemen	Lack of defined roles and responsibilities for IT Risk Management	Lack of defined roles and responsibilities for IT/cyber Risk Management Limited ref to Risk Management responsibilities within key officer "Role Profiles" Limited in IT Risk Management Policy (OR04) regarding roles and responsibilities. Current Cyber Board ToR (copy we have appears to be a draft) limited with regard to risk management role or responsibility. States will "Review any additional threats or risks identified since last meeting and "Review progress report re delt work to remediate risks identified by NCC-PSN and other cyber threats". A "Cyber Board Action-Decision Tracker" is used by Cyber Board to track decision and actions regarding issues that they are made aware of. These issues/risks or not rated or prioritised so providing limited focus for targeted management based on the level of severity, hindering Cyber Board from operating effectively or efficiently. The Cyber Board ToR does not state that the board will review the IT/Cyber risk register. One of the boards objectives is "To prioritise the risks and agree mitigations to the threats faced". This is a greater challenge without a comprehensive risk register. Cyber board Chair is stated as Strategic Director for Customer and Corporate Services. At time of audit this post was vacant. There is a need for an alternative. At present the SIRO does not attend the Cyber Board. It may be appropriate for this role to attend or chair the Cyber Board. Nothing regarding Risk Management roles and responsibilities in new draft contract between PCC and Delt. Management should review and define the roles and responsibilities regarding IT/Cyber Risk Management and ensure that this is appropriately documented and communicated.	2. Agreed by Management	High	Management accept the observations as set out. Noting that since the audit there is now a consolidated Cyber risk log for consideration at the Cyber Board. Addressing these recommendations will be achieved through the following actions: 1/. Updating the Risk Management Policy OR04 (see above). 2/. Reviewing and updating the Cyber Board ToR including all the roles and responsibilities to ensure adequate coverage from Directors in post. Transformation Architecture Mgr (PH)	Kirsty Harrison (20 October 202	31/10/2025	FULLY IMPLEMENTED	Implementation was completed in December 2025.

This page is intentionally left blank

Audit Area	Audit Name	Recommendation Name	Recommendation Description	Status	Priority	Management Action	Update Notes	Target Implementation Date
Resources Directorate (C	Cyber Governance and Access Management	PCC CGUM22 - User Management Processes Weaknesses	The known weaknesses in the end-to-end user management processes should be identified at the Cyber Board and the risks appropriately managed. The creation of a risk register to provide transparency and a means of governing the associated risks should be considered. Furthermore, the commencing of a workstream/ project to make the necessary improvements would provide a timeline around which some impetus could be achieved.	4. Partially Implemented	High	Cyber board to oversee the implementation of Joiners, Movers and leavers following the principle of Least Privilege as identified by Cyber 360, and the Council's Cyber Risk framework. Target Date: 30/06/2024 Responsible Officer: Cyber Board	2025 10:08): PH - Delt are working towards a unified set of processes to ensure that access permissions for new joiners, movers and leavers are aligned across all IT licences and priveliges and payroll status, based on a set of role based access rights. This work was held up with the implementation of our new payroll system and is now active again. Rob Mitchell (11 August 2025 10:34): Kirsty Harrison (25 July 2025 10:23): Cyber board 26th July - User Access Management improvement plan in progress by Delt, reliant on move to iTrent which took place in June 2025, time required to embed before moving forward with Joiners, Movers, Leavers improvement work. Updates are sought at Cyber Board however associated risks and	30/09/2026

This page is intentionally left blank