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 (I	PCC Cyber Security - Governance (Risk Manageme	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 (I	PCC Cyber Security - Governance (Risk Manageme	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.