Action Reference	Name of Audit	Action	Revised Due Date	Previous Updates	Current Update Narrative	Anticipated Completion
CSTA23/4.1	Cyber Security Training and Awareness 2023/24	1.1 The goal is for 90% of staff to finish the Boxphish training by June 2025	31-Aug-25	• Number of modules has been reduced to prevent information fatigue in the staff. • The training will be spread over 6 weeks as part of a campaign with the assistance with comms. • Discussions underway on progressing this.	The campaign has been launched in collaboration with the communications team, with the first set of training videos scheduled for release before the end of the month. The overall risk level around phishing attempts is expected to decrease once the organisation has completed the initial round of training and we identified users who require additional support or targeted assistance.	Dec-25
CSTA23/4.2	Cyber Security Training and Awareness 2023/24	2.1 The aim is for 80% of councillors to complete the Boxphish training by June 2025.	31-Aug-25	• Linked to CSTA23/4.1 • Number of modules has been reduced • Negotiations with Dem Services required	The campaign referenced in CSTA23/4.1, is designed for staff, and the training content is also intended for use by Councillors. We've been working closely with Democratic Services to design a plan to suit the members requirements and availability. Councillors are frequently targeted by hostile actors due to their visibility in public meetings and their work within the constituencies they represent. It is therefore essential that the training is completed this year to help mitigate the risk of compromise.	Dec-25
CSTA23/4.3	Cyber Security Training and Awareness 2023/24	3.1 ICT will review reports from Boxphish and the Learning Pool to assess current competency levels in cyber security. This review will guide adjustments to the training type and frequency.	31-Aug-25	• Plans for Staff and Members are progressing and are linked to this action.	Since it is not currently possible to directly link reporting data between Learning Pool and Boxphish, we have reached an agreement with HR to use the management reports generated by the Boxphish system as the primary source for evaluating future training needs. These reports will help us monitor user engagement and performance, identify areas where additional support may be required, and ensure that our training strategy remains aligned with organisational goals.	Dec-25
CSTA23/4.4	Cyber Security Training and Awareness 2023/24	4.1 The IT Security and Acceptable Use Policy will be updated in 2024 to inform all staff and councillors that failure to maintain current training for cyber security may result in the loss of IT system access.	31-Aug-25	• AI and Cyber Elements being drafted for peer review	The latest revision of the IT Security and Acceptable Use Policy includes draft guidance on AI usage and updated cyber security measures. It is currently undergoing peer review, with plans to present the draft to SLT for approval in mid-September. This version provides instructions on the responsible use of AI, and its approval will help mitigate the risk of staff inadvertently causing a compromise or data breach due to a lack of awareness.	Oct-25

EEBC - ICT Department - Outstanding Audit Actions 2022-2025 Appendix 1

Action Reference	Name of Audit	Action	Revised Due Date	Previous Updates	Current Update Narrative	Anticipated Completion
CSTA23/4.5	Cyber Security Training and Awareness 2023/24	5.1 Staff knowledge of GDPR and cyber security risks diminishes over time and are at higher risk of causing a cyber security incident through their actions.. Actions to mitigate this risk will be addressed as outlined in sections 3.1 and 4.1.	31-Aug-25	• Progressing as planned	As outlined in the two preceding updates, the work described in section 3.1 (Phishing Reports) and section 4.1 (Updated Acceptable Use Policy) is progressing at pace. This action will be marked as complete once both items have been finalised.	Dec-25
CSTA23/4.6	Cyber Security Training and Awareness 2023/24	6.1 As part of the Boxphish rollout, councillors and staff will undergo simulated phishing exercises. Results will be monitored and evaluated, with additional training offered to those who fail to detect the phishing attempts	31-Dec-25	• Progressing as planned	Linked to the update on CSTA23/4.1, the Boxphish campaign will launch for staff in the first week of September, with rollout to members planned shortly thereafter. Unlike previous cybersecurity and phishing training initiatives, the phishing simulations will begin soon after the training sessions are completed, ensuring timely reinforcement of learning and awareness.	Dec-25
CSTA23/4.8	Cyber Security Training and Awareness 2023/24	8.1The Acceptable Use Policy (AUP) is being revised for re-approval this year. The updated AUP will include a section for signatures, dates, and returns to HR. I	31-Aug-25	• Revision of AUP continues	In connection with the update on CSTA23/4.4, the revised Acceptable Use Policy (AUP) is currently under review, with plans to submit it to the Senior Leadership Team (SLT) for approval in September.	Oct-25
DB24/5	Data Backup and Ransomware Protection	3.1 The mover’s guidance for ICT admins will be reviewed and adapted for a non-technical audience. Once finalised, it will be published on the ICT intranet site later this year, alongside the Starters and Leavers guidance for Managers.	31-Dec-25	• Progressing as planned	This relates to action IA21/3.7, which covers the Starters, Movers, and Leavers process. As part of this activity, it will also explicitly include and document the procedures for maintaining administrative accounts used by the ICT team and specific departments such as Revenues and Benefits who also have nominated technical staff.	Dec-25

Action Reference	Name of Audit	Action	Revised Due Date	Previous Updates	Current Update Narrative	Anticipated Completion
DB24/5	Data Backup and Ransomware Protection	4.1 Creation of an ICT Backup Policy that will align with other ICT Policies that have either already been updated, or due to be updated this year.	31-Dec-25	• Policy creation will align with our existing backup arrangements.	The ICT Backup Policy is currently being drafted and will undergo review with input from service providers and EEBC's security solution partner to ensure it aligns with operational and security requirements.	Dec-25
DB24/5	Data Backup and Ransomware Protection	5.1 A quarterly schedule will be established to test the recovery of systems selected by the team. This testing will take place during the monthly downtime window.	31-Dec-25	• Schedule has been defined and added to the regular downtime tasks.	A schedule has now been defined and incorporated into the routine downtime task list to ensure ongoing consistency and accountability. With this integration complete, the associated action is considered resolved and will be formally closed.	Completed since last update
DB24/5	Data Backup and Ransomware Protection	7.1 Explore additional backup solutions to strengthen overall data protection and ensure continuity in specific operational scenarios.	31-Dec-25	• Discussions have taken place to see if this can be completed with any existing solutions or whether additional hardware or software solutions might be required. • Investigations continue.	Confirmation received that existing solutions will not cover all the identified and recommended requirements. We are currently exploring additional backup solutions to complement the organisation's existing arrangements. This initiative aims to improve overall system resilience, ensure robust long-term data retention, and reinforce business continuity planning.	Mar-26
Db24/5	Data Backup and Ransomware Protection	8.1 The ICT Password Policy whilst updated to cater for PCI compliance will be updated mid-term to cater for the requirements detailed in the NCSC guidance (where practicable).	31-Dec-25	• In-house discussions continue on this topic	Discussions with the internal auditors are scheduled to take place in September to review the policy that was created last year. The aim is to assess its current relevance and determine any necessary updates, with a view to issuing a mid-term revision.	Dec-25
IA21/3.5	Internal Audit Plan 2021/3	1.2- IT Data Management - We are aware the SQL databases are out of support and projects planned for 2022/23 to replace these systems	30-Sep-25	• SQL servers associated with the old Dynamics CRM have been switched off as planned (along with the Application Servers). • There are three remaining servers that are anticipated to be switched off in the coming week before the IT Health Check is started on 28/07/2025	The remaining out-of-support SQL servers have now been successfully decommissioned, completing remediation efforts ahead of the PSN Assessors' visit in September. As such this action will be formally closed.	Completed since last update

Action Reference	Name of Audit	Action	Revised Due Date	Previous Updates	Current Update Narrative	Anticipated Completion
IA21/3.7	Internal Audit Plan 2021/3	3.2- IT information Security - Movers guidance for managers will be created and the entire process reviewed	31-Aug-25	• Linked to action DB24/5 3.1 and DB24/5 9.1	Updated guidance for managers on the Starters, Movers and Leavers (SML) process is currently being drafted. The documentation is undergoing peer review and is scheduled for publication on SharePoint in October. This updated guidance will consolidate existing procedures and provide more detailed documentation of the processes involved, helping to ensure consistency and clarity across all stages of the SML lifecycle	Oct-25
IA21/3.30	Internal Audit Plan 2021/3	3.1- Network M -A Cyber Security Response Plan / Playbook and associated documentation, policies and procedures will be created in conjunction with our SIEM/SOC provider. NCSC and specialist guidance will be sought and followed where appropriate to do so	31-Aug-25	• Meetings have concluded with the SOC provider and a SOW created to understand the scope and costs • Process now needs to move to procurement and if additional suppliers are to be invited to bid an agreement on what we can and cannot share needs to be agreed.	The external Cyber Security providers are currently conducting a comprehensive gap analysis of our existing documentation. This process involves identifying any deficiencies, inconsistencies, or areas that require enhancement to align with best practices and compliance standards. Once the analysis is complete, they will provide a formal response outlining their findings and recommendations. This will include a proposed timeline for when the Cyber Security Response Plan (CSRP) will be available in its first draft form for internal review. Based on current progress, we anticipate receiving this initial draft by late September.	Nov-25
IA21/3.31	Internal Audit Plan 2021/3	4.1- Network Management -A complete set of network documentation will be created/updated in tandem with the deployment of new infrastructure	31-Aug-25	• Work on the documentation continues as planned. • Likely new network design is in draft format that will lead to the creation of a specification that will form part of the procurement process to order kit that needs to be replaced.	While some of the existing documentation remains valid, the cancellation of the planned move to 70 East Street has prompted a redesign of the network infrastructure. As a result, new hardware specifications have been developed, and work is now underway to implement a revised network architecture that reflects this change in direction.	Dec-25
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	DM2.3 –Ex-staff accounts will be removed, and the leaver process will be amended to explicitly include the removal of database accounts.	31-Dec-25	• Linked to action DB24/5 3.1 and DB24/5 9.1	The action to remove ex-staff accounts has been documented within the ICT process library, alongside the leavers process, to ensure that administrative access is also revoked appropriately. This documentation will be incorporated into the broader Starters, Movers, and Leavers (SML) framework for the entire organisation, as outlined in actions DB24/5 and IA21/3.7. As far as this specific action is concerned this can be formally marked as completed.	Completed since last update

EEBC - ICT Department - Outstanding Audit Actions 2022-2025 Appendix 1

Action Reference	Name of Audit	Action	Revised Due Date	Previous Updates	Current Update Narrative	Anticipated Completion
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	DM3.1 We will implement an SCCM patch exception report that will list when patches have not been successfully applied. This will be run at downtime and exceptions will be investigated by the Infrastructure Team.	31-Jul-25	• Server likely to be decommissioned before the end of August 2025.	SCCM has now entered the decommissioning phase and has been replaced by a Microsoft cloud-based solution for server management. This new platform includes robust patch management and comprehensive reporting capabilities. As a result, this action is considered complete and will be formally closed.	Completed since last update
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	DM5.1 – Formal change control procedure document, to include backout plans and other good practices will be created and circulated to all ICT staff	31-Aug-25	• Process for a new Change Advisory Board is being created to complete this action. • Likely this will sit with an ICT Wide Ops Board to replace the previous one that predominantly dealt with infrastructure matters.	Change Management is now incorporated into the ICT Team Site, with supporting documentation being added as required. Although the framework is still evolving, it currently captures both standard and emergency changes and facilitates a structured approval process.	Nov-25
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	NM1.2 – A redesigned network will be implemented. Expert advice will be sought to inform and assure that business requirements are captured and addressed, and the design adheres to appropriate security standards.	31-Oct-25	• Linked to IA21/3.31	As outlined in the update to action IA21/3.31, the revised network design and its components have been reviewed following the cancellation of the planned move to 70 East Street. While some existing documentation remains applicable, the change in location has necessitated a further redesign of the network infrastructure. Procurement is now underway to source the updated hardware required to support the new configuration.	Dec-25
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	DM1.2 - The SQL databases are out of support and projects planned for 2022/23 to replace these systems	31-Jul-25	• Most of the SQL servers that were the source of this action have been replaced, upgraded or removed. There are three final servers that are due to dealt with before the ITHC takes place in the week commencing 28/07/2025	Per IA21/3.5 - The remaining out-of-support SQL servers have now been successfully decommissioned, completing remediation efforts ahead of the PSN Assessors' visit in September. As such this action will be formally closed.	Completed since last update
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	DM6.1 – Monthly test of database backups will be performed as part of monthly maintenance weekend.	31-Aug-25	• This process has been discussed within the Infrastructure team and a process developed to evidence that testing has taken place.	This process has now been integrated into the monthly downtime checks and is considered complete. Accordingly, the associated action will be closed.	Completed since last update

Action Reference	Name of Audit	Action	Revised Due Date	Previous Updates	Current Update Narrative	Anticipated Completion
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	NM1.4 Network monitoring will be reviewed and improved. Implementation will be a phased deliverable of the rolling programme of network upgrades	31-Aug-25	• Issues with the reports have been raised with Zabbix and a follow up will take place in September.	The reporting function is now capable of generating reports on demand, providing flexibility for ad hoc analysis and operational oversight. However, the availability of regular scheduled reporting remains limited at this stage. As such this action is considered complete and will be closed.	Completed since last update
IA24/5 ITFOLLOW UP	Follow Up Reviews of Data Management and Network Management	NM1.6 – Change Management will be reviewed and formalised. Consideration will be given to including this within the monthly Operations Board or as a standalone activity	31-Aug-25	• Linked to IA24/5 ITFOLLOWUP • Process for a new Change Advisory Board is being created to complete this action.	This is referenced in action DM5.1, and the associated process is currently undergoing a trial phase prior to formal adoption. The trial aims to validate its effectiveness and ensure it meets operational requirements before being fully integrated into standard practice.	Nov-25
LS23/4.1	Legacy Systems	1.1 As part of the works to move the organisation to 70 East Street a complete review of the legacy systems is underway. This will be reported to SLT along with mitigations by the end of March 2025.	30-Sep-25	• Works on this have been delayed due to the Application Manager leaving the authority. The sudden passing of another key member of ICT staff this year has compounded this. • The cancellation of the move to 70 East Street means that there are some minor changes to the application estate, but these will not be impactive. • Revised review will be completed with the two new-in-post managers in ICT with a view to sharing this with SLT in September 2025	The current legacy infrastructure comprises six software systems, three of which are actively being migrated to new, compliant replacement systems. In addition, legacy hardware—including the thin client solution previously deployed at EEBC—is in the process of being phased out. A detailed list of these systems will be provided to SLT in a separate report to support ongoing oversight and planning for their decommissioning or replacement.	Oct-25
LS23/4.4	Legacy Systems	4.1 Action taken in 1.1 will mitigate this risk (Failing to provide a complete list of legacy IT systems will lead to an inability to have a thorough overview of the inherent risks)	30-Sep-25	• As noted in the update to LS23/4.1 this updated list of applications and mitigations will be presented to SLT in September 2025	Related to 1.1 - systems have now been identified across both hardware and software domains, and mitigation plans are actively underway to address these elements. A detailed report outlining these systems and the associated actions will be presented to SLT in mid-September.	Oct-25