Appendix 2: Closed /implemented Audit Actions closed since April 2022

Area	Agreed Action	Report Audit opinion
Cyber Security Risk Management 2020.21 / 4	Management should undertake a review to assess the content, delivery method and quality of the council's user education programmes for cyber/IT security. Efforts should be made to harmonise the education packages, extracting the most relevant elements from each to create an optimum package. Due to increased security concerns as a result of COVID-19, the awareness training should be focused on phishing emails and social engineering. This education should be deployed to users at least on an annual basis, with consideration given to bu-annual refresher sessions. New starters must complete this education on a mandatory basis to ensure that security awareness is embedded from day one of their employment within the Councils. Training completion should be monitored and there should be a record of all the training that has been provided and completed to all members of staff.	Limited
Cyber Security Risk Management 2020.21 / 6	Management should ensure that the migration plans of unsupported Windows system is recorded and tracked to completion. It should also be included within the Council's ICT Risk Register and take steps to decommission these devices as soon as possible.	Limited

Cloud Computing 2020.21 / 3	Management should determine the agreed criteria to be used when assessing an application's potential for migration to the cloud. Using the Applications Matrix as guidance, a defined framework should be constructed to ensure that all potential scenarios are factored into the assessment criteria to determine the driving focus. For example, an application may be identified as nearing the end of its support agreement, so the potential to amend its current hosting methods may be preferable for reasons such as cost, system availability or system stability. Alternatively, the hardware used to host the application may be due for replacement, so a decision must be taken on whether migration to the cloud is a preferable option. The design of the framework should be consistent, yet flexible enough to adapt to multiple potential scenarios, at its core, focusing on the elements regarded as high priority, such as: cost saving, potential risk, system availability and contractual obligations. The key element of the decision-making process is to assess the appropriateness of migrating/not migrating an application to the cloud versus remaining "as is", with clearly documented pros and cons of each scenario.	Limited

Cloud Computing 2020.21 / 4	Using the Migration Assessment Framework as a guide, a Corporate Applications Roadmap should be drafted, to ensure which applications the Councils would migrate to the cloud as well as which must be migrated to the cloud (for example, to avoid an impending required investment such as procurement of a new hardware.) Management should assess possible dependencies of each system moving forwards, considering that multiple services may exist on the same platform on multiple servers – including business critical with non-business critical - so what happens to one application may impact others hosted on the same server. The Corporate Applications Roadmap should have a forward projected “review by” date applied for all systems that cannot be migrated to the cloud at this time and an overview of dependencies prohibiting migration, with a schedule to revisit and reassess their status built into ICT’s ongoing calendar of activities. In addition, there should be reviews performed for all applications that have already been migrated to the cloud to evaluate latency and user connectivity, system availability, and if the hosting method remains appropriate.	Limited
Access Management Control 19.20 / 5	Head of IT & Digital 3C Shared Services should ensure requirements for setting up new user access to the network are set out in formal policy document and is uploaded onto the intranet and the PPMS. Line managers acknowledge the formal policy set out by 3CSS which ensures £CSS are notified of leavers in timely manner.	Adequate
Hardware & Software Asset Management Control 19/20 / 3	A thorough review of the ICT asset database should be undertaken on a regular basis to ensure that all assets include a location and the information recorded on them is complete, accurate and up to date.	Adequate

Hardware & Software Asset Management Control 19/20 / 5	Management should perform an exercise to gather licensing information evidence relating to all the business and IT software applications. Additionally, licensing information should be recorded but not limited to : - Licence type - Product keys (if applicable) - Locations of the installation CD - Licence expiry	Adequate
Hardware & Software Asset Management Control 19/20 / 6	There should be a mechanism in place to monitor and review software installed on all end point devices.	Adequate
Protocol Policy Management System 18.19 / 3	Management will put a plan in place to seek staff awareness of IT policies by including a rolling awareness programme for extant policies within the protocol policy management system.	Adequate
Network System Resilience & Availability 19.20 / 1	Management should establish planned schedule for testing of data centre failover. Testing should be undertaken on at least an annual basis.	Adequate
Purchase Order Compliance 2019.20 / 1	Investigation into what can be done within the system to place a lockdown on budget codes so only budget manager and their delegated officers can use their cost centre and approve expenditure on their code. This investigation will also find out what HDC can amend alone and what can be done with Tech1 assistance (and the cost of this). Investigation should also look at whether the system can be set so that the PO originator defaults to sending the PO to the budget holder i.e. link a user to a default approver.	Limited
Purchase Order Compliance 2019.20 / 3	Authorisation limits will be reviewed – unlimited authorisation limits will be amended; and users will be given appropriate limits based on needs for their role (not their grade) and the existing hierarchy within their team and who should be authorising POs.	Limited
Purchase Order Compliance 2019.20 / 4	Self -authorised requisitions will be monitored. The process by which this will be done is yet to be decided: it is likely to be a 6 monthly report of activity and volume, and check and re-education.	Limited

Purchase Order Compliance 2019.20 / 6	The above user guidance will include specific guidance on the use of retrospective ordering (when it is appropriate/efficient to use). Consideration will also be given to introducing a Performance Indictor for retrospective ordering to measure its ineffective usage and inform where further education is needed.	Limited
Purchase Order Compliance 2019.20 / 7	Guidance will also include the use of ‘bulk orders’ which can be used for contracts requiring repeated invoices over the year introducing draw-down from the total commitment. This will be set-up and users provided with education and a demo on its use and application within Services.	Limited
Purchase Order Compliance 2019.20 / 8	Investigation will be made into finding out how many supplier accounts we have for employees and put these accounts into suspension so they cannot be used.	Limited
Budget Monitoring and Forecasting 2020.21 / 1	Management should perform a training needs analysis to identify and assess the level and type of training required by members of staff with regards to budget monitoring and forecasting and the use of the forecasting module, which should include, but not be limited to, salaries and project budgets. A mandatory training programme should be put in place that is based upon the requirements of the training needs analysis. Training completion should be recorded and monitored and training should be maintained for audit purposes.	Substantial
Budgets and MTFS 2020.21 / 2	Management should document the Council's MTFS methodology, which should include, but not limited to: - The documentation required and used during the process - Interviews with key personnel undertaken - Risk assessments - Information gathered and used, including the basis for assumptions	Adequate

Treasury Management 2020.21 / 1	Management should put arrangements in place for ensuring that investment opportunities outside the Council's Treasury Management are identified and proactively monitored. Furthermore, the Council should put in place detailed and defined guidance with regards to any such investment opportunities with clear linkages to the Council's Treasury Management Strategy and framework.	Adequate
Treasury Management 2020.21 / 2	Management should finalise the Terms of Reference for the Council's Treasury and Capital Management Group, which should ensure that the Group provides sufficient oversight and monitoring of the Council's treasury management activities. Furthermore, the Terms of Reference should define the frequency with which the Group should meet and there should be a requirement for action plans to be put in place and followed up to resolution.	Adequate
Cyber Security Risk Management 2020.21 / 1	Management should provide operational updates including risk status related to its compliance with National Centre for Cyber Security (NCSC) 10 Steps for Cyber Security Principles (such as Network Security, Secure Configuration, Incident Management and Malware Prevention) to the information Governance Group on a quarterly basis to ensure all key stakeholders are engaged and aware of current status.	Limited
Cyber Security Risk Management 2020.21 / 2	Management should complete the update of the Council's Information Security Policy and ensure that it is communicated to all staff. A section should be included to provide adequate guidance for users regarding the secure usage of mobile devices/laptops/phones to reduce the risk of misuse/potential loss or theft/confidential data exposure.	Limited

Cyber Security Risk Management 2020.21 / 3	Management should complete the update of the Council's Cyber Security Incident Response Plan. The plan's contents should reflect the guidance provided by the NCSC (National Cyber Security Centre) and include the following: - Procedures for assessing the nature and scope of an incident - Identifying an incident - Eradication procedures - Containment procedures - Recovery - Lessons learnt All stakeholders must be aware of their roles and responsibilities and the document should be included in a regular review cycle, at least once per year.	Limited
Digital Services - Development and Management 2020.21 / 2	The Matrix should be used as a primary source of reference throughout ICT and potentially the wider business, detailing key information about systems integration, application management and maintenance, documenting all integration journeys into and out of the system and key dependencies, as well as support arrangements, the hosting platform, and system life-cycle management information. Additional information should also be added to the Applications Matrix in due course, such as designated system Data Stewards and System Administration/Super User information.	Adequate
Digital Services - Development and Management 2020.21 / 3	Business processes should also be adapted to ensure that the Applications Matrix is consulted prior to making changes or decisions about hosting methods. The matrix may evolve into an essential reference point, but its usage needs to be embedded into existing practices to ensure the matrix remains of value.	Adequate
Digital Services - Development and Management 2020.21 / 4	Management should provide guidance to all Service Areas who own and manage their own applications, informing them that any changes made to systems which integrate with other systems and services must be communicated to ICT, with an explanation of potential impacts, such as integration breakages.	Adequate

Digital Services - Development and Management 2020.21 / 5	ICT should provide guidance to operational teams on how Service Areas may utilise test environments, and provide information about the existing processes for undertaking changes, particularly with reference to the weekly Change Advisory Board meetings. This flow of information should be supported by designated points of contact within both the teams and ICT to maintain open lines of communication.	Adequate
Digital Services - Development and Management 2020.21 / 6	Systems that have integration should be flagged within the Application Matrix so that the Councils know that a process must be followed and communicated to ICT if a change is required. Operational teams should obtain access to the Matrix (or a cut-down version of it that cannot be edited) which should be consulted prior to any changes being made. If a required change is identified for one of the systems that is flagged, it should be communicated to ICT, who should provide guidance and support to ensure the change does not impact systems.	Adequate
Digital Services - Development and Management 2020.21 / 7	Focusing on Active Directory accounts and access to high risk applications such as payroll, financial and procurement, a review of all users with access should be performed to confirm there is a continued business need. The Leavers' Process should be updated to include checking that all application-level access is revoked when someone leaves the Council.	Adequate
Digital Services - Development and Management 2020.21 / 8	Additionally, as a secondary control to identify when errors are made during execution of the Council's Leavers' process, a review should be performed every 90 days/each quarter to identify any Leavers' AD accounts that still remain in an active state. Steps should then be taken to disable/remove that access as soon as possible.	Adequate
Digital Services - Development and Management 2020.21 / 9	Management should ensure that the configurations for the integration failure email alerting system is documented, particularly how errors are identified and managed, with the potential of improving the process, or perhaps investing in additional alerts in the future. The process should be documented and shared with all relevant staff.	Adequate
Main Accounting System 2020.21 / 1	The Disaster Recovery Plan will be reviewed and updated to reflect the move to Tech1 and any revised arrangements to ensure continuity of service across the wider Finance area.	Adequate

Debtors 2020.21 / 1	Systems, processes and resource needs will be reviewed across the whole Debtors function. An action plan will be established, in conjunction with the team, to support delivery of improvements and address the control failings identified during the quarterly reviews (see Appendix, attached to the action).	Limited
Creditors 2020.21 / 2	Written procedure notes will be reviewed and updated to ensure that they are reflective of current practices and cover all elements of the creditors system	Adequate
Creditors 2020.21 / 3	The Supplier Amendment Form (SAF) will be updated to include the requirement for Tech1 to be checked for existing suppliers prior to the new supplier being requested. In addition, AP staff will be reminded of the need to check the system before a new supplier is created.	Adequate
Creditors 2020.21 / 4	Options for monitoring and addressing duplicate payments will be investigated and staff (AP team and wider services) will be reminded of the checks required when processing invoices for payment.	Adequate
Cloud Computing 2020.21 / 1	Management should review and revise the ICT Strategy document to include a detailed overview of intentions to perform feasibility assessments on corporate applications/services to ensure if they can be potentially hosted in the cloud.	Limited
Cloud Computing 2020.21 / 2	Management should update the design of the ICT Applications Matrix to include a detailed profile of each corporate application in use throughout the three councils. The matrix should contain information about the application, such as: - how it is supported and by whom - where it is hosted - what contractual obligations are in place - whether a system upgrade is pending and it has vendor agreement to be hosted in the cloud. As well as supporting a defined framework criteria for assessing applications' optimum hosting platforms, this document will also inform business continuity planning and future decisions for enhancement or replacement of applications.	Limited

MiPermit 2021.22 / 3	In conjunction with the Information Governance Manager / Data Protection Officer, consider what information may need to be added to the MiPermit Portal to highlight the Privacy Notice to customers before they submit their information.	Adequate
Inventory of IT Assets 2021.22 / 1	Run regular reports from 'lansweeper' to establish what assets are connected to employee's laptop and update the inventory with this information. This will be dependent on speaking with the system administrator of 'lansweeper' to establish if docking stations could also be detected on the software. Dependent on the success of Lansweeper, further inventory review may need to take place via Microsoft forms, in which employees' detail what equipment employees have in their custodianship. [Discussions held regarding wording so not to highlight that ICT are unaware of location and custodianship of hardware]	Limited
Inventory of IT Assets 2021.22 / 2	Previous Hardware & Software Asset Management Control 19/20 audit resulted in the creation of Action 1516: "A thorough review of the ICT asset database should be undertaken on a regular basis to ensure that all assets include a location and the nformation recorded on them is complete, accurate and up to date". This action remains in process. The current audit highlights that this action cannot be closed as a review of the inventory has not been conducted and no process in place to ake the review regular. This should be completed once the Inventory is up to date following the reviews.	Limited
Inventory of IT Assets 2021.22 / 3	Conduct a 'Laptop Amnesty' to collect unused laptops from staff. This is to then be followed by a 'walk around' Pathfinder House, checking cupboards and drawers to gather unused laptops. Update the inventory where necessary.[Discussions held egarding wording so not to highlight that ICT are unaware of location and custodianship of hardware]	Limited
Inventory of IT Assets 2021.22 / 4	Update the Asset Tagging Process to include: An independent officer to run a monthly report to ensure the number of assets ordered via Tech1 reconciles with the number of assets uploaded into the inventory for the same month. Any discrepancies eed to be reported. [An independent officer should be someone separate from the officers who received the order at Pathfinder House and uploaded the assets into the inventory].A process to create an entry in the inventory to record asset tag 'errors'and gaps and provide an explanation as to why an asset number is not assigned to an asset. This should be followed with retraining staff of the new asset tagging process.	Limited

Inventory of IT Assets 2021.22 / 6	Reminder to all staff of the ICT Asset Management policy so they are aware of how to request and update location of assets through hornbill and also how to appropriately return assets.[This was previous Action 1515 from Hardware & Software Asset Management Control Audit 19/20. Closed 21/12/2020 but now has lapsed]	Limited
Inventory of IT Assets 2021.22 / 7	Review of the custodianship of surplus laptops so they can be readministered within the Council. Ensure that any decisions regarding the custodianship is reflected in the leavers process.	Limited
Inventory of IT Assets 2021.22 / 8	Create policy regarding the donation of ICT assets to communities. This needs to outline what assets can be donated, the criteria for who may receive donated assets and who can authorise the donation. A process also needs to be produced alongside his to confirm how applications for assets can be made and how approval is given.	Limited
Overtime 21.22 Action 4	Overtime claim guidelines will be included in the revised ESS and MSS guidance documents which will be shared with staff and managers as part of the system upgrade. Guidance will include: - general rules for overtime (in line with our existing overtime policy - authorisation requirements - claim timescales (within 90 days of hours worked) - the need to provide a reason for the hours worked - expectations of managers approving claims	Adequate
Overtime 21.22 Action 5	Reports of temporary variations to pay will be reviewed each month. The Payroll Processing Checklist (signed and saved as PDF) will be date stamped as evidence of the check and the report held on file for reference.	Adequate
Overtime 21.22 Action 6	Excessive hours / ask of employees will be incorporated into the Council's future Workforce Strategy, to support our consideration of staff wellbeing.	Adequate
Main Accounting System 21.22 Action 1	The Interim Finance Manager will review reconciliations performed by the Financial and Treasury Accountant. Reconciliations performed for Payroll and Debtors will be reviewed by a member of the Finance team.	Adequate

Main Accounting System 21.22 Action 2	Larger value items in the Cashiers Suspense Account will be reviewed, evidenced as such, and corrected where possible.	Adequate
Debtors 21.22 Action 1	The Credit Control Manager will develop a timetable for key debtor tasks and debt recovery actions, this will be shared with the team and used to direct duties and activity.	Limited
Debtors 21.22 Action 2	The Credit Control Manager will establish a programme of routine meetings with Service Managers to review debt lists.	Limited
Debtors 21.22 Action 3	Monthly management information and debt collection performance data will be prepared and reviewed to support the ongoing monitoring of activity and workload.	Limited
Creditors 2021.22 / 1	Once procedure notes have been completed and finalised, thoroughly review these with the team so they are following the same process and procedure. Ensure that the outcome from transformation has been considered when writing the procedure notes. Please also communicate the procedure across the organisation with the aim that all officers are following the same process and procedure.	Adequate
Payroll - Payments 22.23 / 6	Managers to be advised that as part of an establishment check for 'Ghost Employees' they should review their budgets packs and analyse the employees listed within this to ensure that the details are correct and no unknown officers are listed, and no leavers/new starters present when should not be.	Adequate

Actions closed since last report

Purchase Order Compliance 2019.20 / 2	Further investigation will be taken to find out whether the system can be improved by showing the approver the remaining budget at the time of approving a requisition. This will enforce informed commitment making and remove existing blind approvals.	Limited

Payroll - Payments 22.23 / 1.1	Update timesheet documents so that the data replicates the information needed for input in iTrent.	Adequate
Payroll - Payments 22.23 / 2	Investigation into direct input of timesheets by employees should be undertaken to see if it is a viable option. Benefits of efficiency savings (through not duplicating input and lower risk of transposing errors) needs to be weighed up against any costs of access rights and implications on contracts.	Adequate

56 Actions

3 closed since last report
3 reopened since last report