Appendix 2: Full Detail of Overdue Audit Actions June 2022

Audit Name	Priority Level	Action Detail	Fixed Target	Last Update	Last Update Detail	Service Area
Data Protection and Information Management 15.16	Amber	The Senior Information Risk Officer (SIRO) shall decide how long information and emails etc shall be kept within Anite, and the process for purging or archiving.	30/09/16	17/05/21	The action around I@W was passed to the SIRO following the departure of the previous SIRO. Progress since then has been delayed, but by no means halted by Covid response. Currently the Information and Governance Board at HDC have commissioned a full stock take of information governance arrangements across the authority which has been presented to Corporate Governance and are working through an action plan. In addition policies are being reviewed and adopted as an authority. This work will provide the specific answer to the retention rules for I@W.	Corporate Team
PCI DSS 18.19 / 3	Amber	A training needs assessment should be performed for all members of staff that have responsibility for PCI DSS compliance activities so as to determine their training needs.	01/04/20	20/06/22	HDC's approach has been to mitigate our noncompliance by taking training actions, and stopping call recordings. However, these are mitigations while we work towards full compliance, they do not make us PCI complaint. Any staff member who takes payments are trained as part of being given access to Capita. However, for HDC to be PCI complaint we either have to: •Stop customer card details entering our network (including being spoken to advisors even when calls are not recorded) via technical solutions and integrations •Create a separate accredited network where staff can take card details (thought to be undesirable) •Allow card details to enter our network but make the whole 3C network PCI compliant (considered impractical \ staff resource heavy and costly) HDC is operating some payment systems like Gladstone (for Leisure) which require the customer to speak their card details to a Leisure agent while they are input into a chip and pin machine run in a 'card holder not present mode'. Integrating Gladstone into an IMS would be one option. So HDC's current position is we are working with outside specialists from the NCC Group alongside City and SCDC to document every route to full compliance and then decide on the appropriate one. The implications of doing nothing will also be specified. The Capita IMS contract is coming to an end next year, so PCI compliance is being considered alongside the tender for a new IMS. One option from NCC report could be including PCI compliance measures for all systems in the new IMS	Chief Operating Officer

PCI DSS 18.19 / 4	Amber	Compliance should be monitored and actin taken when members of staff are found to have not completed the PCI DSS training or have not read the policy and procedures.	01/04/20	20/06/22	HDC's approach has been to mitigate our noncompliance by taking training actions, and stopping call recordings. However, these are mitigations while we work towards full compliance, they do not make us PCI complaint. Any staff member who takes payments are trained as part of being given access to Capita. However, for HDC to be PCI complaint we either have to: •Stop customer card details entering our network (including being spoken to advisors even when calls are not recorded) via technical solutions and integrations •Create a separate accredited network where staff can take card details (thought to be undesirable) •Allow card details to enter our network but make the whole 3C network PCI compliant (considered impractical \ staff resource heavy and costly) HDC is operating some payment systems like Gladstone (for Leisure) which require the customer to speak their card details to a Leisure agent while they are input into a chip and pin machine run in a 'card holder not present mode'. Integrating Gladstone into an IMS would be one option. So HDC's current position is we are working with outside specialists from the NCC Group alongside City and SCDC to document every route to full compliance and then decide on the appropriate one. The implications of doing nothing will also be specified. The Capita IMS contract is coming to an end next year, so PCI compliance is being considered alongside the tender for a new IMS. One option from NCC report could be including PCI compliance measures for all systems in the new IMS	Chief Operating Officer
PCI DSS 18.19 / 5	Amber	Actions need to be drawn together in a policy which sets out how the council will manage PCA DSS compliance activities and the policy should be reviewed on a regular basis. this should include but not be limited to: - Assignment of roles and responsibilities for ensuring that the Council is PCS DSS compliant - Procures for staff that are responsible for taking card payments - The Council's security strategy in relation to the storage, processing and transmission of credit card data - A set of instructions for detecting, responding to the storage, processing and transmission of credit card data.	01/04/20	20/06/22	HDC's approach has been to mitigate our noncompliance by taking training actions, and stopping call recordings. However, these are mitigations while we work towards full compliance, they do not make us PCI complaint. Any staff member who takes payments are trained as part of being given access to Capita. However, for HDC to be PCI complaint we either have to: •Stop customer card details entering our network (including being spoken to advisors even when calls are not recorded) via technical solutions and integrations •Create a separate accredited network where staff can take card details (thought to be undesirable) •Allow card details to enter our network but make the whole 3C network PCI compliant (considered impractical \ staff resource heavy and costly) HDC is operating some payment systems like Gladstone (for Leisure) which require the customer to speak their card details to a Leisure agent while they are input into a chip and pin machine run in a 'card holder not present mode'. Integrating Gladstone into an IMS would be one option. So HDC's current position is we are working with outside specialists from the NCC Group alongside City and SCDC to document every route to full compliance and then decide on the appropriate one. The implications of doing nothing will also be specified. The Capita IMS contract is coming to an end next year, so PCI compliance is being considered alongside the tender for a new IMS. One option from NCC report could be including PCI compliance measures for all systems in the new IMS	Chief Operating Officer

Protocol Policy Management System 18.19 / 3	Amber	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.	01/06/20	15/06/22	Update on evidence - This is with HR service to action. Alternative if not possible by end of July 2022 then ICT will recommend this risk is accepted with alternative manual methods (i.e email) of recording staff acknowledgement of policy. Monthly update from HR is that they are still working on how to add the AUP to Itrent and prove staff have read this.	3C ICT
Access Management Control 19.20 / 5	Amber	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.	31/08/20	15/06/22	Monthly update from HR is that they are still working on how to add the AUP to Itrent and prove staff have read this.	3C ICT
Hardware & Software Asset Management Control 19/20 / 3	Amber	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.	01/09/20	09/06/22	Extract of Hornbill database has been done to complete a 20% review of stock and being written into inventory process to ensure this is completed on a quarterly basis. Will upload review once completed, eta 24/06/2022	3C ICT
Network System Resilience & Availability 19.20 / 1	Amber	Management should establish planned schedule for testing of data centre failover. Testing should be undertaken on at least an annual basis.	31/10/20	15/06/22	We will be testing this process at the end of July as part of NSX project. We will close this action and provide evidence of CAB schedule showing work.	3C ICT
Purchase Order Compliance 2019.20 / 8	Amber	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.	30/04/21	10/06/22	Systems Accountant been diverted to managing AP/AR team due to problems the section is experiencing	Corporate Resources
Treasury Management 2020.21 / 1	Amber	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.	10/06/21	17/06/22	The opportunities will be documented in the TCMG meeting summaries (both those rejected and progressed) as part of business as usual.	Corporate Resources
Purchase Order Compliance 2019.20 / 1	Amber	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.	30/06/21	07/03/22	Have discussed with System Accountants at City & SCDC. This would be a major piece of work to re-configure the process and not likely to be done in the near future. Costings not obtained from T1 yet.	Corporate Resources
Purchase Order Compliance 2019.20 / 2	Amber	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.	30/06/21	10/06/22	Meeting arranged for 15th June to see if we can set it up	Corporate Resources
Land Charges 18.19 / 3	Amber	Written procedures should be in place to support how the costs and calculation process is carried out.	30/06/21	10/06/22	The current process for justifying land charge fees is cumbersome, and in my opinion, unnecessarily complicated. This opinion is shared by the current land charges service manager. The current spreadsheet used was created several years ago, and has been refined by subsequent finance staff, but there is still alot of information which is not finance based which has to be provided by the service. I have asked the current land charges manager to make enquiries of other local authorities as to the method they use, but I am unsure whether this has happened yet. As such, I am unwilling to expend resources writing process notes for something which may change imminently	Corporate Resources

Cyber Security Risk Management 2020.21 / 6	Red	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.	31/07/21	09/06/22	*Audit reopened after follow up work found only partially implemented. No update provided by action owner*	3C ICT
Creditors 2020.21 / 3	Amber	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.	31/07/21	31/01/22	Form not yet amended to reflect details agreed, but work is in hand to move to an e-form for new suppliers and supplier changes. It is intended that this will include reference to the checks required, and if possible with incorporate a built-in check to the system for duplicates (requires investigation).	Corporate Resources
Purchase Order Compliance 2019.20 / 5	Amber	Written procedures on the PO process will be written and issued to users. Users will be educated and refreshed on certain areas not being performed correctly and causing delays or inefficiencies in the process e.g. current issue of failure to receipt, inappropriate use of retrospective ordering. Guidance will give specific reference to use of retrospective ordering; correct VAT codes; use of the delegation functionality to avoid delays; etc. Guidance should be posted to the 'Popular' section of the Intranet for quick access for users.	30/09/21	31/01/22	Presentation made at services forum and includes some do's and don't's These procedures have been produced and shared via a number of channels. Guidance is on Slide 5 of this deck… https://councilanywhereorg-my.sharepoint.com/:p:/g/personal/justin_andrews_huntingdonshire_gov_uk/EeSkq4icJ0VKvYNKhogV6vsBizP-Kviu8WFIXDh82NNSzQ?e=w4JWER	Corporate Resources
Purchase Order Compliance 2019.20 / 6	Amber	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.	30/09/21	31/01/22	Action reassigned to Sandra Dean - action transferred with implementation date already passed and no extension provided.	Corporate Resources
Purchase Order Compliance 2019.20 / 7	Amber	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.	30/09/21	31/01/22	Action reassigned to Sandra Dean - action transferred with implementation date already passed and no extension	Corporate Resources
Cyber Security Risk Management 2020.21 / 2	Amber	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.	30/09/21	15/06/22	Update on evidence - This is with HR service to action. Alternative if not possible by end of July 2022 then ICT will recommend this risk is accepted with alternative manual methods (i.e email) of recording staff acknowledgement of policy. Monthly update from HR is that they are still working on how to add the AUP to Itrent and prove staff have read this.	3C ICT

Cyber Security Risk Management 2020.21 / 3	Amber	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.	30/09/21		*no update provided by action owner*	3C ICT
Cyber Security Risk Management 2020.21 / 4	Red	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.	30/09/21	20/04/22	example of up to date/ new content for cyber security training	3C ICT
Main Accounting System 2020.21 / 1	Amber	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.	30/09/21	10/06/22	BCP for TechOne part of overall Finance BCP which has been issued to relevant users to update for their modules	Corporate Resources
Main Accounting System 2020.21 / 3	Amber	The Payroll reconciliation will be remapped / worked up for the new HR / Payroll system. Instructions will be documented and the routine task handed over to the Payroll team for actioning.	30/09/21	15/06/22	Action has now been handed over to the Payroll Manager who is in the process of confirming and documenting reconciliation processes and will then be completing them each month - copies will be passed to the Interim Finance Manager (or a member of her team) for review.	Corporate Resources
Creditors 2020.21 / 4	Amber	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.	30/09/21	13/01/22	reassigned to Sandra Dean , TL of Credit Control Team, as Oliver Colbert no longer in that role/team.	Corporate Resources
Purchase Order Compliance 2019.20 / 4	Amber	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.	31/10/21	10/06/22	Looking to develop report so that it can be produced automatically and send to Managers on a monthly basis	Corporate Resources

Treasury Management 2020.21 / 2	Amber	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.	31/10/21	17/06/22	Meeting summaries identify actions and decisions from the text of the meeting (see summary in item 2). This allows actions to be followed up more easily at the next meeting	Corporate Resources
Budget Monitoring and Forecasting 2020.21 / 1	Amber	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.	31/12/21	03/03/22	This is currently low on the list of priorities, with the 2020/21 audit currently underway, and 2021/22 year fast approaching. Upcoming staffing changes in line management and lack of clarity around roles and responsibilities mean that this has fallen behind schedule.	Corporate Resources
Budgets and MTFS 2020.21 / 1	Amber	Management should perform a training needs analyses to identify and assess the level and type of training required by members of staff and Members with regards to the MTFS and the use of the budget module, which should also identify any training needs for Members. 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 records should be maintained for audit purposes.	31/12/21	03/03/22	This is currently low on the list of priorities, with the 2020/21 audit currently underway, and 2021/22 year fast approaching. Upcoming staffing changes in line management and lack of clarity around roles and responsibilities mean that this has fallen behind schedule.	Corporate Resources
Digital Services - Development and Management 2020.21 / 7	Amber	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.	31/12/21	15/06/22	Because the HR integration / feed in to AD is delayed due to the HR project running behind, 3C ICT have implemented an interim process and procedure involving running monthly reports and then the IT_SD taking specific action to check and disable accounts where staff have left but managers have not notified ICT. This action can be closed once screen shots of the 2 last monthly reports are provided.	3C ICT
Digital Services - Development and Management 2020.21 / 8	Amber	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.	31/12/21	20/04/22	IT_SD to request report from HR on the first working day each month for all leavers for the previous 4 weeks. Output of that report to be cross referenced against AD accounts and hornbill requests logged - Exceptions to be dealt with by IT_SD TL. Evidence / screen shots have been requested from the IT_SD to provide to be included here.	3C ICT
Budgets and MTFS 2020.21 / 2	Amber	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	31/03/22	30/03/22	With the lack of s151 officer, department re-organisation, 2020/21 audit and now 2021/22 year end upon this will not be completed by the target date. I cannot give a revised date at this time.	Corporate Resources
Main Accounting System 2020.21 / 4	Amber	Debtors reconciliation issues will be investigated and resolved. The process for the reconciliation going forward will be documented and responsibility handed over to the Exchequer Officer.	31/03/22	15/06/22	Advised by SRS that reconciliation will be undertaken by her each month	Corporate Resources

Debtors 2020.21 / 1	Amber	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).	31/03/22	10/06/22	The review of AP and AR is currently underway. Following yet another change in line management, this now falls within my remit. The income manager has been temporarily removed from BAU and tasked with ensuring that the Estates income is up-to-date and processes are documented with agreed responsibilities both in the service and Finance. To my knowledge this has been done, and we are now entering a period of embedding the new processes, which should result in more accurate and timely invoices.	Corporate Resources
Creditors 2020.21 / 2	Amber	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	31/03/22		*no update provided by action owner*	Corporate Resources
Small Works Contract 21.22 / 1	Amber	A dedicated small works contract or framework agreement will be tendered and formalised for use across the authority.	30/04/22		*no update provided by action owner*	Corporate Resources
Small Works Contract 21.22 / 2	Amber	Staff responsible for procurement will be made aware of the contract, its use mandated, and details of pricing / rates and staff responsibility will be communicated.	31/05/22		*no update provided by action owner*	Corporate Resources
Inventory of IT Assets 2021.22 / 4	Amber	Update the Asset Tagging Process to include:	31/05/22		*no update provided by action owner*	3C ICT