Public
Key Decision - No

HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter:	Implementation of Internal Audit Actions
Meeting/Date:	Corporate Governance Committee – 26th January 2022
Executive Portfolio:	Executive Councillor for Corporate Services Councillor David Keane
Report by:	Deborah Moss, Internal Audit Manager
Ward(s) affected:	All Wards

Executive Summary:

Key performance indicator: 100% of audit actions to be implemented by the agreed date. Not achieved.

Performance in the last 12 months* to 10th January 2022:

24 actions implemented - 24% on time, increasing to 44% when including late implementation

30 actions not implemented – 56%

(actions due before the last 12 months period are not included)*

37 overdue audit actions remained outstanding at 10 Jan 22.

Recommendation:

It is recommended that the Committee consider the report and comment as they consider necessary.

1. PURPOSE OF THE REPORT

1.1 To update members on the implementation of audit actions.

2. WHY IS THIS REPORT NECESSARY?

2.1 At past meetings of the Corporate Governance Committee (CGC), the committee has expressed concerns at the underachievement of the management-set target of implementing 100% of agreed internal audit actions on time. This report provides an update for members based on audit actions that are outstanding as at 10th January 2022.

It is intended (resources permitting) that a verbal update of current figures will be provided at the January CGC meeting.

3. BACKGROUND

3.1 Following each audit review, audit conclusions, associated actions and implementation dates are agreed between the audit client and the audit team. Services can disagree with any action and the audit report is a record of what has been agreed by way of actions and their target dates.

3.2 The target for the implementation of 'agreed internal audit actions to be introduced on time' is set at 100% in line with best practice that suggests that all recommendations are implemented by the agreed deadline. The deadline date is set/agreed with the client service and can be extended upon request where reasonable justification is provided (the measurement is taken against the new target date). Therefore, it is reasonable that all actions should be completed by their target date.

3.3 For the 12 months ending 10th January 2022, 54 audit actions were due to be implemented. The following shows the performance against due dates:

- 24% (13 actions) were "implemented on time"; this increases to
- 44% (24 actions) when late implementation is also included

- 30 actions (56%) have not been implemented.

Performance % has deteriorated since the last reported figures.
Services have received less individual push from the IAM since the last performance report as it is not considered good use of Audit resource to pursue managers to complete agreed actions; this is a responsibility of Senior Management and Committee.

4. NON-IMPLEMENTATION OF AUDIT ACTIONS

4.1 Sometimes non-implementation of an action is due to operational circumstances and to reflect this, a process is in place for re-assessing an action's implementation date and extending it where reasonable. Even after the introduction of this process the 100% indicator is still not being achieved.

All such extensions are agreed between the audit client and the Internal Audit Manager. Such audit actions are then not considered as "not implemented" and are excluded from the performance reporting unless the new target has also been missed (measurement is taken against variable target date).

4.2 However, circumstances sometimes prevail such that extended deadlines are missed and the current practice is that non-implementation at this stage is reported to management and CGC.

4.3 As at the 10th January 2022, 37 audit actions remained outstanding (overdue) and not implemented. This includes all overdue actions (not just those due in the last 12 months) to give a more accurate reflection.
A detailed analysis of these actions – providing original and variable deadlines - is shown in the **Appendix.**

Of the 37 actions:

- 1 action 2 years or older
- 6 actions are between 1 and 2 years overdue
- 6 actions are between 6 months and 1 year overdue
- 24 actions are less than 6 months overdue

** Time is measured from the 'original target implementation date' to the 10th January 2022.*

4.4 All overdue actions continue to be reported to the SLT through our monthly Risk & Controls Board report. All SLT members are provided with a list of outstanding actions with a request that they ensure their Service Managers implement them. Officers with actions assigned to them have direct access to the system to enable them to manage those actions.

5. KEY IMPACTS

5.1 It is important that the Council maintains a sound internal control environment. Actions that the Internal Audit Service propose to address risk and control weaknesses are discussed with Heads of Service and, if appropriate, Directors and agreement is reached as to any corrective action that needs to be taken. Internal audit actions are not imposed on management or Services.

5.2 An action that is not implemented means that the weakness or risk originally identified in the audit report, and which the action was designed to address, will remain as a risk to the organisation.

6. LINK TO THE CORPORATE PLAN

6.1 The Internal Audit Service provides independent, objective assurance to the Council by evaluating the effectiveness of risk management, control, and governance processes. It identifies areas for improvement across these three areas such that Managers can deliver the Corporate Plan objectives as efficiently, effectively and economically as possible.

7. RESOURCE IMPLICATIONS

7.1 There are no direct resource implications arising from this report.

8. REASONS FOR THE RECOMMENDED DECISIONS

8.1 The report has been requested by the Committee and as such, they need to decide what further action they wish to take.

9. LIST OF APPENDICES INCLUDED

Appendix 1 – Overdue Audit Actions as at 10th January 2022 Summary and Detailed List

BACKGROUND PAPERS

Audit actions contained within the 4Action system

CONTACT OFFICER

Deborah Moss – Internal Audit Manager
Tel No: 01480 388475
Email: deborah.moss@huntingdonshire.gov.uk

Appendix 1: Overdue Audit Actions @ January 2022

Summary:

Audit Name	Variable Target	Fixed Target	Status	Service Area	Priority Risk Level	months late
3C ICT Actions						
Access Management Control 19.20 / 5	31/08/2020	31/08/2020	In Progress	3C ICT	Amber	16
Cloud Computing 2020.21 / 1	31/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
Cloud Computing 2020.21 / 2	31/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
Cloud Computing 2020.21 / 3	31/12/2021	31/12/2021	In Progress	3C ICT	Red	0
Cloud Computing 2020.21 / 4	31/12/2021	31/12/2021	In Progress	3C ICT	Red	0
Cyber Security Risk Management 2020.21 / 1	31/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
Cyber Security Risk Management 2020.21 / 2	30/09/2021	30/09/2021	In Progress	3C ICT	Amber	3
Cyber Security Risk Management 2020.21 / 3	30/09/2021	30/09/2021	Not Started	3C ICT	Amber	3
Cyber Security Risk Management 2020.21 / 4	30/09/2021	30/09/2021	In Progress	3C ICT	Red	3
Cyber Security Risk Management 2020.21 / 5	31/05/2021	31/05/2021	In Progress	3C ICT	Red	7
Digital Services - Development and Management 2020.21 / 7	20/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
Digital Services - Development and Management 2020.21 / 8	20/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
Digital Services - Development and Management 2020.21 / 9	20/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
Protocol Policy Management System 18.19 / 3	30/11/2020	01/06/2020	In Progress	3C ICT	Amber	19
Hardware & Software Asset Management Control 19/20 / 3	31/12/2020	01/09/2020	In Progress	Please Select, 3C ICT	Amber	16
COO Actions						
PCI DSS 18.19 / 3	01/04/2020	01/04/2020	Not Started	Corporate Director - People	Amber	21
PCI DSS 18.19 / 4	01/04/2020	01/04/2020	In Progress	Corporate Director - People	Amber	21
PCI DSS 18.19 / 5	01/04/2020	01/04/2020	In Progress	Corporate Director - People	Amber	21
Director, People Actions						
Data Protection and Information Management 15.16	31/07/2018	30/09/2016	In Progress	Corporate Team	Amber	64

AD, Corporate Services Actions						
Budget Monitoring and Forecasting 2020.21 / 1	31/12/2021	31/12/2021	Not Started	Corporate Resources	Amber	0
Budgets and MTFS 2020.21 / 1	31/12/2021	31/12/2021	Not Started	Corporate Resources	Amber	0
Creditors 2020.21 / 3	31/07/2021	31/07/2021	Not Started	Corporate Resources	Amber	5
Creditors 2020.21 / 4	30/09/2021	30/09/2021	In Progress	Corporate Resources	Amber	3
Land Charges 18.19 / 3	30/06/2021	30/06/2021	In Progress	Corporate Resources	Amber	6
Main Accounting System 2020.21 / 2	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
Main Accounting System 2020.21 / 3	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
Main Accounting System 2020.21 / 5	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
Purchase Order Compliance 2019.20 / 1	30/06/2021	30/06/2021	Not Started	Corporate Resources	Amber	6
Purchase Order Compliance 2019.20 / 2	30/06/2021	30/06/2021	Not Started	Corporate Resources	Amber	6
Purchase Order Compliance 2019.20 / 3	31/07/2021	31/07/2021	Not Started	Corporate Resources	Amber	5
Purchase Order Compliance 2019.20 / 4	31/10/2021	31/10/2021	Not Started	Corporate Resources	Amber	2
Purchase Order Compliance 2019.20 / 5	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
Purchase Order Compliance 2019.20 / 6	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
Purchase Order Compliance 2019.20 / 7	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
Purchase Order Compliance 2019.20 / 8	30/04/2021	30/04/2021	In Progress	Corporate Resources	Amber	8
Treasury Management 2020.21 / 1	31/12/2021	10/06/2021	In Progress	Corporate Resources	Amber	7
Treasury Management 2020.21 / 2	31/10/2021	31/10/2021	Not Started	Corporate Resources	Amber	2

TOTAL 37

* ”Not started” means that no update has been entered on the system by the Service/owner of the action.

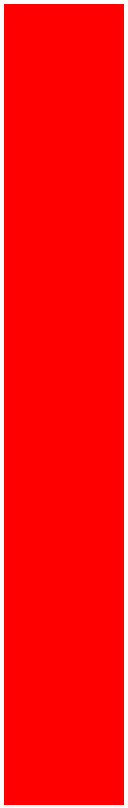
Detail of Actions:

Ref	Audit Name	Action Detail	Variable Target	Fixed Target	Status	Service Area	Priority Risk Level	months late
3C ICT Actions								
1513	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.	31/08/2020	31/08/2020	In Progress	3C ICT	Amber	16
1601	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.	31/12/2021	31/12/2021	Not Started	3C ICT	Amber	0

1602	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.	31/12/2021	31/12/2021	Not Started	3C ICT	Amber	0

1603	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	31/12/2021	31/12/2021	In Progress	3C ICT	Red	0

cloud versus remaining “as is”, with clearly documented pros and cons of each scenario.



1604	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.	31/12/2021	31/12/2021	In Progress	3C ICT	Red	0

1575	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. Management should complete the update of the Council's Information Security Policy and ensure that it is communicated to all staff.	31/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
1576	Cyber Security Risk Management 2020.21 / 2	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.	30/09/2021	30/09/2021	In Progress	3C ICT	Amber	3

1577	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.	30/09/2021	30/09/2021	Not Started	3C ICT	Amber	3

1578	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.	30/09/2021	30/09/2021	In Progress	3C ICT	Red	3

1579	Cyber Security Risk Management 2020.21 / 5	Management should track the ongoing reduction of Domain Administrator accounts. Best practice is to have only 8-10 domain administrators. Privileged network accounts should be reviewed on a regular basis to ensure the number of accounts is controlled and managed appropriately.	31/05/2021	31/05/2021	In Progress	3C ICT	Red	7
1588	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. 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.	20/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
1589	Digital Services - Development and Management 2020.21 / 8		20/12/2021	31/12/2021	Not Started	3C ICT	Amber	0

		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.						
1590	Digital Services - Development and Management 2020.21 / 9	The process should be documented and shared with all relevant staff.	20/12/2021	31/12/2021	Not Started	3C ICT	Amber	0
1526	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.	30/11/2020	01/06/2020	In Progress	3C ICT	Amber	19
1516	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.	31/12/2020	01/09/2020	In Progress	Please Select, 3C ICT	Amber	16
COO Actions								
1529	PCI DSS 18.19 / 3	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.	01/04/2020	01/04/2020	Not Started	Chief Operating Officer	Amber	21
1530	PCI DSS 18.19 / 4	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.	01/04/2020	01/04/2020	In Progress	Chief Operating Officer	Amber	21

1531	PCI DSS 18.19 / 5	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.	01/04/2020	01/04/2020	In Progress	Chief Operating Officer	Amber	21
Director, People Actions								
1137	Data Protection and Information Management 15.16	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.	31/07/2018	30/09/2016	In Progress	Corporate Team	Amber	64
AD Corp Services Actions								

1570	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.	31/12/2021	31/12/2021	Not Started	Corporate Resources	Amber	0
1571	Budgets and MTFS 2020.21 / 1	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.	31/12/2021	31/12/2021	Not Started	Corporate Resources	Amber	0

1599	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.	31/07/2021	31/07/2021	Not Started	Corporate Resources	Amber	5
1600	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.	30/09/2021	30/09/2021	In Progress	Corporate Resources	Amber	3
1568	Land Charges 18.19 / 3	Written procedures should be in place to support how the costs and calculation process is carried out.	30/06/2021	30/06/2021	In Progress	Corporate Resources	Amber	6
1593	Main Accounting System 2020.21 / 2	Alternative Tech1 user roles will be formalised and assigned for the Senior Exchequer and Risk Officer and the Reconciliations Officer, to ensure that permissions and access levels are appropriate and relevant to the role.	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
1592	Main Accounting System 2020.21 / 3	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.	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
1595	Main Accounting System 2020.21 / 5	Responsibility for reviewing and actioning the Cashiers Suspense Account each year will be reassigned.	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3

1545	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. 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.	30/06/2021	30/06/2021	Not Started	Corporate Resources	Amber	6
1546	Purchase Order Compliance 2019.20 / 2	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.	30/06/2021	30/06/2021	Not Started	Corporate Resources	Amber	6
1547	Purchase Order Compliance 2019.20 / 3	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.	31/07/2021	31/07/2021	Not Started	Corporate Resources	Amber	5
1548	Purchase Order Compliance 2019.20 / 4		31/10/2021	31/10/2021	Not Started	Corporate Resources	Amber	2

1549	Purchase Order Compliance 2019.20 / 5	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. The above user guidance will include specific guidance on the use of retrospective ordering (when it is appropriate/efficient to use).	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
1550	Purchase Order Compliance 2019.20 / 6	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. 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.	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3
1551	Purchase Order Compliance 2019.20 / 7	This will be set-up and users provided with education and a demo on its use and application within Services.	30/09/2021	30/09/2021	Not Started	Corporate Resources	Amber	3

1552	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. Management should put arrangements in place for ensuring that investment opportunities outside the Council's Treasury Management are identified and proactively monitored.	30/04/2021	30/04/2021	In Progress	Corporate Resources	Amber	8
1573	Treasury Management 2020.21 / 1	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. 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.	31/12/2021	10/06/2021	In Progress	Corporate Resources	Amber	7
1574	Treasury Management 2020.21 / 2	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.	31/10/2021	31/10/2021	Not Started	Corporate Resources	Amber	2

TOTAL 37

Overdue Audit Actions									
Ref	**Audit Name and Action Number**	**Assignee**	**Action / Risk Priority**	**Detail**	**Evidence to be Provided**	**Current Due Target**	**Original Target Date**	**Status**	**Time lapse since original date (months)**
1137	Data Protection and Information Management 15.16 / 10	Oliver Morley		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. *The SIRO role was transferred on the departure of the previous incumbent late 2019, and the role reassigned the Corp Director (O Morley).*	Decision taken and copy of instruction informing managers.	31/07/2018	30/09/2016	NotStarted	39
1529	PCI DSS 18.19 / 3	Oliver Morley		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.	Shared Service Management Board minutes	01/04/2020	01/04/2020	NotStarted	12
1530	PCI DSS 18.19 / 4	Oliver Morley		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.	Shared Service Management Board minutes	01/04/2020	01/04/2020	NotStarted	8

1531	PCI DSS 18.19 / 5	Oliver Morley		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.	Shared Service Management Board minutes	01/04/2020	01/04/2020	NotStarted	9
1526	Protocol Policy Management System 18.19 / 3	Madelaine Govier		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.	High level plan.	30/11/2020	01/06/2020	NotStarted	18

1513	Access Management Control 19.20 / 5	Sagar Roy		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 3CSS are notified of leavers in timely manner.	User access policy or requirements in an equivalent policy. Acknowledgement from line managers and employee owners.	31/08/2020	31/08/2020	InProgress	18
1516	Hardware & Software Asset Management Control 19/20 / 3	Colin Chalmers		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.	Review of records highlighted by BDO. Supporting evidence - written confirmation that task to review location records has been completed,	31/12/2020	01/09/2020	InProgress	18
1552	Purchase Order Compliance	Claire Edwards		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.	IA to be advised of outcome.	30/04/2021	30/04/2021	NotStarted	0

1540	IT Maintenance Schedule Planning 20.21 Action 2	Alex Young		"Management should update the published Business Applications matrix to document which team/third party vendor is responsible for the management of security update patches/version upgrades."	"Updated Business Applications matrix."	31/07/2021	31/07/2021	InProgress	1
1545	Purchase Order Compliance 2019.20 / 1	Claire Edwards		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.	Claire Edwards to provide details to IA of what investigation has been carried out and its conclusions.	30/06/2021	30/06/2021	NotStarted	1
1546	Purchase Order Compliance 2019.20 / 2	Claire Edwards		This investigation will also find out what HDC can amend alone and what can be done with Tech1 assistance (and the cost of this).	Details to be advised to IA	30/06/2021	30/06/2021	NotStarted	0
1547	Purchase Order Compliance 2019.20 / 3	Claire Edwards		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.	Evidence of review and outcomes.	31/07/2021	31/07/2021	NotStarted	3
1568	Land Charges 18.19 / 3	Claire Edwards		Written procedures should be in place to support how the costs and calculation process is carried out.	Procedure notes to be completed and uploaded to action before closure.	30/06/2021	30/06/2021	InProgress	1
1579	Cyber Security Risk Management 2020.21 / 5	Alex Young		Management should track the ongoing reduction of Domain Administrator accounts. Best practice is to have only 8-10 domain administrators.	It is acknowledged that work is underway to reduce the number of Domain Administrator	31/05/2021	31/05/2021	NotStarted	2

					accounts, but a target date should be set for when the validation exercise is due for completion, with regular reporting in place to monitor the decrease in number.				
1580	Cyber Security Risk Management 2020.21 / 6	Alex Young		Management should ensure that the migration plans of unsupported Windows system is recorded and tracked to completion.	A defined roadmap should be produced to outline the total number of systems which will be decommissioned and by what date, and progress status reports should be produced and shared with key stakeholders.	31/07/2021	31/07/2021	NotStarted	0
1581	Cyber Security Risk Management 2020.21 / 7	Alex Young		Management should put a procedure in place to apply anti-malware signature updates to devices that do not connect to the Council's IT network on a routine basis. This should include a process to restrict any non-complying devices connecting to the Council's IT network.	ICT is currently assessing each endpoint to validate the extent of the outdated agent and as part of that exercise should any device be found to be severely out of date, it must be investigated further and, if deemed to be a risk, prohibited from accessing the network until it is compliant.	31/05/2021	31/05/2021	NotStarted	2

1599	Creditors 2020.21 / 3	Sandra Dean		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.		31/07/2021	31/07/2021	NotStarted	0

TOTAL 17