INTERNAL AUDIT REPORT

Area of Review	IT controls
Contact Officer	Internal Audit Manager
Date	February 2022
Version	Final

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

1. BACKGROUND

1.1 As part of the 2021-22 Internal Audit Plan, a review of the key controls for IT has been undertaken.

1.2 Responsibility for IT controls for centralised systems lie with the Head of Corporate Services, with the day to day administration and management of IT controls being the responsibility of the IT Manager. Responsibility for IT controls for devolved systems lie with the relevant Head of Service and System Administrators.

1.3 It is important to note that a sample of cloud based hosted systems were chosen within this review. These were the Zellis, Uniform and Arbitas systems. The Corporate Network was also reviewed.

2. SCOPE OF THE REVIEW

2.1 We have reviewed the policies and processes in place for officers to ensure that IT controls are complied with. We have performed walkthrough testing, where appropriate, and assessed the effectiveness of internal controls to ensure that risk is managed effectively.

2.2 Specific elements of the review have included:

- IT systems access
- GDPR
- Cyber security

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

3. CONTROL OBJECTIVES

3.1 The scope of this review has encompassed the following control objectives:

Control Objectives	
1	That all IT system access controls are managed effectively.
2	That Data held on IT systems complies with the requirements of GDPR.
3	That there are adequate business continuity and emergency response measures in place in the event of a cyber security attack

4. AUDIT APPROACH

4.1 Our audit approach to this review has been to:

- Obtain and understand the relevant processes through discussions with key personnel, review of systems documentation and perform walkthrough tests where appropriate.
- Identify the key risks within the function.
- Evaluate and test the effectiveness of the controls in place to address these risks.
- This review has been undertaken in compliance with the Internal Audit Public Sector Standards 2017.

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

5. OPINION ON CONTROL FRAMEWORK

5.1 The overall level of opinion that can be provided on the internal control framework over the Corporate IT network and applications controlled by the Corporate IT service is:

Levels of Assurance	
Substantial	Substantial assurance given where there is a sound system of controls in place, which applied consistently to enable achievement of the intended objective.
Satisfactory	Satisfactory assurance given where there is generally a sound system of internal control in place with only minor lapses, and in general, objectives achieved.
Limited	Limited assurance is given where controls in place are not always applied and objectives may not be achieved, meaning the Council is exposed to the risk of financial loss, fraud or the loss of reputation.
None	No assurance is given where weaknesses in control has resulted if a failure to achieve objectives

5.2. The level of assurance provided for IT applications managed outside of the Corporate IT function is limited. Levels of assurance are based on the key findings summarised in paragraph 5.4.

5.3 This report seeks to highlight some of the main issues and assist in the development of an improvement plan. There is one high risk, seven medium risk and two low risk recommendations.

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

5.4 Key areas requiring improvement for the Abritas, Uniform and Zellis applications include:

- Governance; including roles and responsibilities.
- Users access including; consistency of process and temporary staff/agency access
- Cyber attack recovery documentation
- National Cyber Security Centre advice and guidance, in particular their public sector cloud security guidance.
- GDPR and cyber security training for temporary / agency staff.

In addition, other areas for improvement include;

- Polices and Written Procedure Notes
- Third party access particularly around the AD accounts through the key internal control of reconciliations

5.5 A request was made to the contractor for information to give assurances that it had been requested by the Council's IT section for appropriate personnel to be removed, where required, that this had occurred. However, no response has to this date, been received.

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

6. SUMMARY OF IDENTIFIED RISKS AND RECOMMENDATIONS TO BE AGREED WITH MANAGEMENT

#	Risk	Issue identified	Risk Assessment	Recommendation	Management Response / Mitigation	Responsible Officer	Target Date
1	There may be unauthorised access to the council's data which could lead to a financial risk through non-compliance with GDPR regulations.	That system administrators are not always made aware of leavers. Examples of this were identified in Uniform and Abritas.	Medium	Appropriate devolved systems that stand outside of the corporate network should be included in the new starter and leaver process to ensure that they are all captured.	This was recognised and IT will identify systems and will work through ensuring that managers are notified.	IT Manager	February 2022
2.	IT risks may not be identified, assessed, analysed and mitigated if they are not included in the appropriate governance	There are no clearly defined responsibilities for service areas to adhere to in respect of expected IT access controls,	High	There should be clear guidelines given to managers / systems administrators to ensure that they are fully aware of their responsibilities. This should include:	It was agreed at Leadership team 01/03/2022 that the IT manager and the Information Governance Officer will set up meetings with the	Leadership Team	June 2022

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

	documentation, I.e., the service risk registers.	security, management and cyber security of the Arbritas, Uniform and Zellis systems including identification and documentation of risks,		Reconciliation of system administrators System access management of agency / temporary staff System administration management and review Inactivity report monitoring Actions to be taken in the event of a Cyber attack Consideration to be given to reviewing and updating job descriptions Adhere to NCSC security guidance	administrators of the devolved systems and address the control / cyber / GDPR requirements to ensure compliance. Procedure notes will be produced to document the controls required and these procedures will be circulated to Managers and system administrators		
3	Without Electronic Written Procedure Notes, there is no point of reference for staff to refer to	There are no electronic written procedure notes for the new starter and	Medium	There should be electronic written procedure notes in place to support the new starter and leaver	This will be discussed with HR to ensure that it is included.	IT Manager	March 2022

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

	in the event of a query.	leaver process for the network.		process recently introduced.	Managers have been told on numerous occasions that the new IT form is the new process		
4	Systems may not have the facility for disabling inactive accounts after a set number of days if it is not stated as required in the IT Security Policy which could put the Council's data at risk.	Whilst accounts are disabled when they are inactive after a set number of days, there is no mention in the IT Security Policy or IT Access Policy that accounts will be disabled where they have not been used after a set number of days	Low	It should be recorded within the appropriate policies that accounts will be disabled if inactive for a set number of days and that this is actioned.	This is noted – there are a number of systems used with the authority with different timescales. This is a process being worked through. Systems identified and integrated in to Azure ID	IT Manager	Ongoing
5	Without a formal reconciliation of the active directory and other IT systems managed in service areas there is the risk of unauthorised	Hart IT reviews on a quarterly basis the active AD accounts. A follow up review found that	Medium	That AD checks are documented and actions to remove users are followed up and documented.	Quarterly checks are completed by Hart IT this is reviewed and anomalies	IT Manager	Ongoing

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

	access to the network and non compliance of GDPR	despite a request for users to be removed they had not been. Audit trails of these checks were not always available			highlighted with Capita.		
6	There would be no readily available source of reference. Without controlled policy documents, duties and responsibilities could become confused and/or not operated.	Corporate documents held on Sharepoint for staff to refer to are controlled by the author who sets the permissions themselves and staff and management may not be aware of this	Medium	It should be clearly stated within an appropriate policy to ensure that staff and managers are aware of their responsibilities with regard to putting corporate documents on to Sharepoint.	Reminders and guidance should be given to officers	IT Manager	March 2022
7	There is a risk to the Council and personal data if controls have not been considered for new IT systems.	It was established that the current Housing system is being decommissioned with a new	Medium	It is recommended that controls are reviewed as part of the project plan prior to implementation and once the new system is built that the controls	A Meeting has been arranged between the IT manager and the Housing System project manager to ensure that the	Housing	March 2022

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

		system being built. A number of documents relating to controls was requested. The system administrator stated that this information will be used to help build the processes and procedures in the new system.		are reviewed to ensure they are effective and efficient. Should the new system not be up and running then the controls should be incorporated into the current system.	key cyber and IT controls are included in the project implementation. The Information Governance Officer is involved in the project and will continue to advise on best practice.		
8	Without an up to date PSN assessment and accreditation Hart's data may be at risk.	At the time of testing the latest PSN report was dated January 2020, which contained 2 high risk vulnerabilities and 2 low risk the vulnerabilities.	Medium	A PSN assessment should be undertaken at the earliest time.	During the audit it was explained that a PSN assessment has been booked in for w/c 4th Oct and the on-premises ones are scheduled for 2nd November. As of 07th December 2021 Hart Council will no longer require		Closed

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

					to submit a PSN assessment to Cabinet Office due to services being migrated to the public internet.		
	GDPR						
9	Governance is weakened if not all required data is input into the Data Audit sheets	There are Data Audit sheets in place for all directorates and they are mainly completed. However, there are instances where cells are not completed and the header is not filled in for the Controller.	Low	Data Audit sheets should be complete.	Most of the information for the incomplete cells is not applicable. For example, the Data Audit sheets are not used for logging personal data breaches. These are recorded in the Incident Register. However, there is an action in the UK GDPR Project Plan to complete the cells. Although information about the Controller needs to be added to the Data	Information Governance Officer	April 2022

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

					Audit sheets, it is already held elsewhere i.e., in data processing and sharing agreements, registers etc. However, there is an action in the UK GDPR Project Plan to complete the header for the Controller.		
10	Council data may not be dealt with in line with GDPR legislation and requirements leaving the council of financial and reputational risk.	It was explained that there are gaps regarding appropriate training for agency staff for GDPR or cyber security as they do not officially get picked up and there is nothing written down.	Medium	Agency staff should have appropriate training on GDPR and cyber security.	Current agency staff attended a UK GDPR briefing on 22/11/2021. In future, HR will provide the Information Governance Officer (for GDPR training) and the IT Client Officer and the Audit Manager (cyber security training) with the details of any agency staff who start with the	Information Governance Officer / IT Client Officer and Audit Manager	Completed (for GDPR training)

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

					Council so that they are invited to training.		

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.