No.	HOS	Director	Code	Audit Title	Assurance	Priority	Audit Finding	Recommendation	Status 10 Sept 2024	Revised Due Date	Closed Date
1	T.Tudor	K.Dove	1819 App cont 02	IT Application Controls	~~Limited~~ Reasonable	Medium	The specific responsibilities of system administrators in regard to managing local IT applications is not documented and hence they may be unaware of what the role entails.	System administrator responsibilities should be documented and communicated.	This will be documented by the due date	30-Sep-24	
2	T.Tudor	K.Dove	1819 App cont 03	IT Application Controls	~~Limited~~ Reasonable	Medium	The corporate Access Control Policy states that user access rights should be granted on the basis of business need and documented in an access control statement, held by the person or team that manages the system. Our testing identified that a documented access control statement does not exist for the majority of IT applications	A template access control statement should be devised and completed for each IT application.	This will be documented by the due date	30-Sep-24	
3	T.Tudor	K.Dove	1819 App cont 04	IT Application Controls	~~Limited~~ Reasonable	Medium	For the majority of IT applications, users are locally based and hence system administrators are aware of any leavers and take action to disable their accounts. Some system administrators use the leaver information within the monthly newsletter for this purpose. However, some IT applications are accessed beyond the local service area and administrators do not receive any formal notification of staff leavers. From the IT applications tested, this includes iWorld, Civica, Exacom and Objective. The Oracle Financials system is hosted externally at Solihull Metropolitan Borough Council and user management is undertaken by IT Services. However, there has been no recent review to confirm that all users are valid.	A process should be put in place to ensure all IT system administrators receive notification of staff leavers. In addition, a review of the users on the Oracle Financials system should also be undertaken.	Close - Single Sign On is the preferred and implemented standard for identity management across primary and new applications. Key risk has been addressed.	30-Sep-24	
4	T.Tudor	K.Dove	1819 App cont 10	IT Application Controls	~~Limited~~ Reasonable	Medium	None of the service areas, apart from IT Services, has any formal procedures for user management or maintenance e.g. requesting new accounts or making changes to access rights.	Minimum user management and maintenance procedures should be agreed for service areas.	Close - Single Sign On is the preferred and implemented standard for identity management across primary and new applications. Key risk has been addressed.	31-Oct-24	
5	T.Tudor	K.Dove	1819 App cont 11	IT Application Controls	~~Limited~~ Reasonable	Medium	With the exception of the Mitrefinch TMS and Anite IT applications, user access rights are not subject to any regular formal review. On some IT applications the last review was completed over 12 months ago and on others it was over two years ago. No evidence is retained to confirm the reviews undertaken.	All system administrators should be informed to carry out an annual review of user access rights and retain evidence confirming it has been completed.	Close - Single Sign On is the preferred and implemented standard for identity management across primary and new applications. Key risk has been addressed.	31-Oct-24	
6	T.Tudor	K.Dove	2021 ICT Remote Working 08	ICT Remote Working	Reasonable	Low	Section 4.1 of the Acceptable Use Policy states that users should sign a Mobile Device Custodian Form when they are issued with a new device and re-sign it when the device is returned. However, this form is not used. This issue was previously reported in 2017.	The need for the Mobile Device Custodian Form should be reviewed and it either implemented or the AUP updated accordingly.	Close - Mobile Device Form has been implemented		
7	T.Tudor	K.Dove	2021 ICT B&R 01	ICT Backup & Recovery	Reasonable	Medium	There is a new corporate IT backup solution which is in the final stages of implementation. However, we found that supporting documentation for the new solution has yet to be developed. As guidance, the following areas should be covered in the documentation of the new backup solution: • Architectural Summary • Backup Policies • Backup Schedules (times) • Retention Policies • Monitoring and Error Management of Backup Jobs • Cloud Replication	Documented standards, procedures and processes should be developed to support the new IT backup solution and include the areas identified.	Close - Backup processes have been documented		
8	T.Tudor	K.Dove	2021 ICT B&R 08	ICT Backup & Recovery	Reasonable	Low	The three corporate IT policies which cover the backup and recovery of IT systems and data are IT Business Continuity/DR Policy, Cloud Computing Policy and Information Management Policy. A review of these policies found that they all missed their scheduled review on 30 November 2020.	The IT Business Continuity/DR Policy, Cloud Computing Policy and Information Management Policy should be reviewed.	Close - Policies have been reviewed		
9	T.Tudor	K.Dove	2122 M365 07	Microsoft 365	Reasonable	Medium	Data retention policies are not defined for SharePoint or mailboxes.	Data retention policies should be applied to SharePoint and mailboxes and also on OneDrive when it is fully rolled out.	Sharepoint migration project is in-progress. Once complete data retention can be communicated to staff and implemented.	30-Nov-24	
10		K.Dove	2223 GDPR 05	GDPR	Limited	Medium	There is a 'GDPR Compliance' document which defines responsibilities for compliance activities and states that IT will run compliance tools to monitor data retention periods are being adhered to. Discussions with the Information Manager found that tools can only be used on systems where IT have access to the back-end database and, to date, reports have only been run on Uniform for the Environmental Health service. The retention of personal data has not been confirmed in key areas, HR, Revs and Bens and Finance.	An assurance mechanism should be put in place to confirm compliance with the GDPR retention schedule.	Dependent on completion of sharepoint migration project	30-Nov-24	
11		K.Dove	2223 GDPR 08	GDPR	Limited	Medium	There has been a piece of work to identify all data processors and ensure formal agreements/contracts are in place which have the requisite GDPR clauses. The project plan shows this work was fully completed in January 2021. However, the ROPA shows a small number of areas where the existence of an agreement/contract with a data processor is still unknown. A review of the standard contract terms and conditions, along with the associated Annex 9 data processing summary, found they cover the mandatory GDPR clauses, apart from the controller's obligations and rights.	The data processors identified on the ROPA as not having a formal agreement or contract should be followed up and addressed. In addition, the standard contract should include a clause on the controller's obligations and rights.	Task reallocated to current DPO and contracts to be collected and documented in ROPA.	30-Nov-24	
12		K.Dove	2223 IT Disaster Recovery 02	IT Disaster Recovery	Limited	Medium	The ICT Business Continuity Plan has recently been updated by the Information Manager, which is the first update since the covid pandemic. A review of the plan found there is out-of-date information at section 2.2 in regard to having disaster recovery kit at Staffordshire County Council. The plan's version history also suggests it has never been formally approved since it was developed in 2015. Other technical details that are not documented in the plan but may be required to support a recovery, include: •Details of backups and how they can be accessed; •IT systems with failover arrangements at the HIS; •The DNS/firewall changes required to support a recovery performed at the HIS or in Azure; •Network schematic; •List of IP addresses; and •Server specifications.	The ICT Business Continuity Plan should be reviewed and updated to include the areas highlighted, or at least reference where the information can be found. Following this the plan should be formally approved.	Close - BCP reviewed and updated		
13		K.Dove	2223 IT Disaster Recovery 05	IT Disaster Recovery	Limited	Medium	A small number of business critical IT systems are externally hosted, such as Finance and HR/Payroll. These systems should be subject to annual disaster recovery tests by the supplier but this is not verified.	The completion of disaster recovery tests for externally hosted IT systems should be confirmed annually.	Close - tests occur annually		
14		K.Dove	2324 IT Incident Management 01	IT Incident Management	Reasonable	Medium	IT incident management procedures are not documented. ICT Services have an interim arrangement with a third-party, RazorBlue, for first line support services. This comes to an end in January 2024, although there is an option to extend for a further three months.	Incident management procedures should be documented once the long term arrangements for first line support have been agreed.	Long-terrm arrangements for first line approved in August 2024. Processed now to be documented	31-Oct-24	
15		K.Dove	2324 IT Incident Management 02	IT Incident Management	Reasonable	Medium	There are two service desk systems in operation. RazorBlue have their own system for logging support calls and the ICT team continue to use their existing system for tickets that are escalated to them.	The issue of using two separate service desk systems should be resolved.	Close - intregration now in place		
16		K.Dove	2324 IT Incident Management 03	IT Incident Management	Reasonable	Medium	RazorBlue specify a response time for incidents based on their severity level. Response times are not specified for calls passed to the in-house ICT team for resolution.	Service levels should be agreed for calls passed to the in-house ICT team.	Service Levels can be defined in software in new internal service desk platform.	31-Oct-24	

17		K.Dove	2324 IT Incident Management 04	IT Incident Management	Reasonable	Medium	There are 49 open tickets on the internal service desk system. A review found a number are over two months old and the oldest is from March 2023. Open tickets are not subject to any formal review to establish why they have not been progressed. RazorBlue do not report on open tickets on their service desk system.	A formal procedure should be put in place to review all open tickets. This should include tickets on the RazorBlue service desk.	Close - weekly review meetings with Razorblue		
18		K.Dove	2324 IT Incident Management 05	IT Incident Management	Reasonable	Low	Support calls that cannot be resolved by RazorBlue are transferred to the in-house ICT team for resolution. These calls are logged under a general "inquiry/help" category on the service desk.	The category field should be manually updated on tickets that are transferred to the in-house ICT team.	Close - this related to Service Now which has been decommissioned		
19		K.Dove	2324 IT Incident Management 06	IT Incident Management	Reasonable	Low	When a call is passed to the in-house ICT team it is left open on the RazorBlue system so that it can be updated with progress. These updates should happen automatically as activity is logged on the internal service desk, but the process is not working and updates are having to be done manually.	The issue with the automatic updating of tickets on the RazorBlue system should be resolved.	Close - intregration now in place		
20		K.Dove	2324 IT Strategy 01	IT Structure and Strategy	Reasonable	Medium	A draft ICT Strategy has recently been written by the Interim ICT Manager. A review of the strategy found that it includes a number of technology areas, such as networks, infrastructure, end user computing, cloud and anti-virus. There is also reference to cyber security and different certifications and standards. The draft strategy does not include any details on how it supports corporate priorities and objectives or on how it will enhance the customers digital experience. The application section is limited to a number of central ICT applications and the IDOX Uniform products. There are no details on how other corporate business IT applications will be developed. The time period for the ICT strategy is also not defined.	The ICT Strategy should include: •The period of time it covers; •Details on how it supports corporate aims and objectives; •How it will improve the customer's digital experience; •The development of corporate business IT applications. Once updated, the strategy should be formally approved by Leadership Team.	Close - strategy further developed, reviewed at Leadership Team and shared with staff for consulation		
21		K.Dove	2324 IT Strategy 02	IT Structure and Strategy	Reasonable	Medium	The draft ICT Strategy does not have an implementation plan/roadmap associated with it.	An implementation plan should be developed for the ICT Strategy prior to formal approval.	Close - Strategy includes implementation plan		
22		K.Dove	2324 IT Strategy 04	IT Structure and Strategy	Reasonable	Low	An IT steering committee or equivalent group does not exist.	An IT steering committee should be considered for oversight of the ICT service, strategy and key IT projects.	Close - strategy further developed, reviewed at Leadership Team and shared with staff for consulation		
23		K.Dove	2324 Data Breach Management 01	Data Breach Management	Reasonable	Medium	The Council use the GDPR Guru e-learning training module for staff to complete in their induction and annually thereafter. This covers their responsibilities under UK GDPR and information security, including reporting data breaches. To consolidate the learning, staff must achieve at least 80% on the test at the end of the training module. However, we reviewed the staff training completion records and found that only 177 of the 299 staff had completed the training by the required due date. Of the 122 staff (41% of all staff) that had not completed the training: •39 staff have been assigned the module but have not completed it. These are likely to be new staff who have not yet completed the training. •Three staff have their training status as due to be completed in March 2024 but the training does not appear to have been completed. •64 staff showed their training has expired (and is therefore due for refresher training). This includes senior members of staff. •16 staff training records show as being 'overdue', ie the module has been allocated to them but not completed. These training records include staff that are on long term absence (eg sick or maternity leave). However, this level of non-compliance was significantly higher than we would expect. Particularly as it is a mandatory training course and staff are sent reminders electronically to notify them of non-compliance.	The DPO should monitor the training completion report for the e-learning module weekly. Reminders should initially be sent to the staff members, with a separate list reported to the Corporate Management Team showing the non-compliance for each service area. Heads of Service and line managers should then be responsible for ensuring that their team have completed the training module.	Close - this has been implemented		
24		K.Dove	2324 Data Breach Management 02	Data Breach Management	Reasonable	Medium	Data security related incidents, including data breaches, are more likely to occur if appropriate measures are not in place to mitigate the risk of human error. A global risks report published by the World Economic Forum in 2022 found that 43% of all breaches were caused by internal actors (whether intentional or accidental). Therefore, as data processors, communication with staff must be sufficient to ensure they understand their responsibilities for reporting breaches. The mandatory e-learning training module covered data breach reporting. However, we found that 41% of staff had either not completed the module at all or had not completed it in over a year (see Finding 1). Therefore, other communications with staff periodically throughout the year is critical. But, we were informed by the DPO that that corporate communications are not regularly sent to staff to inform them about their responsibilities for reporting breaches. This could be sent to staff through emails or via the Council's intranet page.	The DPO and Corporate Management Team should identify and agree a programme of communications with staff on data breach management through existing corporate communication platforms, such as emails, newsletters, Microsoft Teams notification, the intranet, etc. These could be timed with other national events such as National Data Privacy Week.	Close - regular DPO updates issued to staff		

25		K.Dove	2324 Data Breach Management 03	Data Breach Management	Reasonable	Low	Under Article 33 of UK GDPR, organisations are required to record and monitor both data breaches and any near misses (incidents which are not required to be reported to the ICO) to comply with the accountability principle of UK GDPR. Reportable breaches must be reported to the ICO within 72 hours upon the initial notification of the breach. If a breach is likely to result in a high risk to a data subject's rights and freedoms, then they must be informed of the data breach. Due to the reputational impact that a data breach can cause, it is important that the Council record breaches and near misses and identify any lessons learned from incidents. Between April 2023 and March 2024 there were 14 incidents recorded on the Data Breach Log (one reportable breach and 13 near misses). We reviewed three near misses and one reported data breach to assess whether these were reported to the DPO in a timely manner and processes in accordance with the Council's escalation procedures. Processes were followed and the near misses/data breaches were recorded on the Data Breach Log however, we identified some exceptions: •For one of near misses (DB-23/24-4), a recorded confirmation was not retained on the file to demonstrate that evidence related to the near miss had been destroyed. This would typically be recorded to support the narrative on the Data Breaches Log to evidence that the data has been destroyed. •One data breach related to a loss of customer data by a supplier (DB-23/24-13). The lessons learned and post-incident assessment of data held by third parties was not undertaken to identify safeguards to prevent a reoccurrence of the breach or to obtain assurance over supplier's data storage security arrangements. •The number of data subjects potentially impacted by a near miss was not recorded on the Data Breach Log (DB-23/24-2). Although, this breach related to data left on a printer in the Council's office and, therefore, it was contained internally.	1.The DPO should ensure that reported data breaches and near misses are accurately recorded with sufficient information about the breach and how it was managed on the Data Breach Log. This should include the number of affected data subjects and the category of data involved. 2.For reportable data breaches to the ICO, the DPO should complete a documented post-incident assessment, identifying lessons learned and potential safeguards that can be implemented to prevent a reoccurrence of the incident, even if the ICO has reported that no further action is required. This includes assessing supply chain risks of associated third parties to obtain assurance that the Council's data that is shared with third parties is held securely.	Close - improved data breach recording occurs and evidence captured of decisions		