South Oxfordshire District Council

Listening Learning Leading

Vale of White Horse District Council

Internal Audit Report

Information (Inc. Cyber) Security 2022/2023

SOUTH OXFORDSHIRE DISTRICT COUNCIL
AND
VALE OF WHITE HORSE DISTRICT COUNCIL

Draft issued: 14 October 2022

Final issued: 18 November 2022

Assurance Rating: Limited

CONTENTS

Page

MANAGEMENT SUMMARY

1. INTRODUCTION

1.1 This report details the internal audit review of procedures, controls, and the management of risk in relation to information (inc. cyber) security. The audit has been undertaken in accordance with the 2022/23 internal audit plan agreed with the joint audit and governance committee of South Oxfordshire District Council (South) and Vale of White Horse District Council (Vale). The audit has a priority score of 21. The audit approach is provided in the audit framework in Appendix 1.

1.2 The following objective areas have been covered during the course of this review:

Objective area	Proposed high level scope
Obj1: Policy and procedures	• A cyber/information security framework, policies, and procedures are in place.
Obj2: Training and guidance	• Information security training is delivered to officers and members. • Up-to-date guidance information is available to officers and members and activities to raise awareness of cyber and information security principles and policies are regularly undertaken.
Obj3: Information and security breach reporting	• Am established process is in place for reporting and communicating information security and cyber breaches.
Obj4: Risk management	• Information security and cyber security risks are considered and managed within the corporate risk register, and at a service level within individual service team risk registers.
Obj5: Disaster recovery and business continuity	• A disaster recovery and business continuity plan are in place, up to date and protect the organisation in the event of a major incident. • Back-up routines and security updates are performed in line with agreed contract requirements.

2. PREVIOUS AUDIT REPORTS

2.1 Information (inc. cyber) security was last subject to an internal audit review in November 2020 and seven recommendations were raised. All seven recommendations were agreed, and a limited assurance opinion was issued.

2.2 One recommendation has been implemented, one recommendation has been partly implemented and five recommendations have not been implemented. One recommendation is restated in this review (Rec 3) and four recommendations are no longer applicable.

3. 2022/23 OVERALL AUDIT ASSURANCE

3.1 **Limited assurance:** There are some weaknesses in the adequacy of the internal control system which put the system objectives at risk and/or the level of non-compliance puts some of the system objectives at risk.

3.2 11 joint recommendations have been raised in this review. Six high risk, three medium risk and two low risk.

Objective area	Recommendations		
	Ref	Description	Risk score
Obj1: Policy and procedures	1	IT security policy and procedures	8
	2	Joiners, movers, and leavers (JML) process	8
	3	Cyber security response strategy/plan **(*restated*)**	5
	4	5CP/Capita security policy and procedures	3
Obj2: Training and guidance	5	Training (council employees, agency staff, contractors, and members)	8
	6	Guidance records	5
	7	Employee induction programme	3
Obj3: Information and security breach reporting	One verbal recommendation raised		
Obj4: Risk management	8	LGA audit recommendations	8
	9	Risk registers (services)	5
Obj5: Disaster recovery and business continuity	10	Business continuity plan	8
	11	Back up routines	8

4. BACKGROUND INFORMATION

4.1 Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private, and sensitive information or data from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

4.2 Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

4.3 South and Vale have a statutory duty under the following legislations and associated regulations in relation to the use, storing and handling of information:

- Data Protection Act 2018 and UKGDPR;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004 (EIR);
- Privacy and Electronic Communications Regulations 2003;
- Regularly of Investigatory Powers Act 2000;
- Copyright, Designs and Patents Act 1988;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Counter-Terrorism and Security Act 2015;
- Protection of Children Act 1978;
- Criminal Justice and Immigration Act 2008;
- Criminal Justice and Immigration Act 2008;
- Defamation Act 2013;
- Equality Act 2010;
- Terrorism Act 2006;
- Limitation Act 1980;
- Official Secrets Act 1989;
- Malicious Communications Act 1988;
- Digital Economy Act 2010;
- Privacy and Electronic Communications Regulations 2011;
- Police and Justice Act 2006;
- Obscene Publication Act 1964;
- Police and Criminal Evidence Act 1984;
- Prevention of Terrorism Act 2005.

4.4 The councils' IT services, including IT/Cyber security, was outsourced on the 1 August 2016 to Capita, as part of the five councils' partnership (5CP). Capita have a service delivery plan (SDP) and service specification (SS) for the services they provide and have developed a specific plan for IT security. The SDP and SS describes the service that will be carried out for the five councils under contractual agreements signed by all participating parties, including for IT (cyber) security controls.

4.5 The councils also hold contractual agreements with a number of IT service providers of cloud-based applications, including Unit4, LoneAlert and Zellis (ResourceLink). The management of IT security and disaster recovery routines for these applications falls outside the direct responsibility of the councils and Capita.

4.6 The government's National Cyber Security Centre (NCSC) defines a cyber security incident as:

- A breach of a system's security policy to affect its integrity or availability; and/or
- The unauthorised access or attempted access to a system that
  a) actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes; or
  b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Such incidents could be either intentional or accidental in nature but can be determined by the root cause.

4.8 Examples of cyber security incidents may include, but not limited to un-targeted and targeted cyber-attacks. Un-targeted cyber-attacks, attackers indiscriminately target as many devices, services, or users as possible. To do this, they use techniques that take advantage of the openness of the internet, which include:

- **phishing** - sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website;
- **water holing** - setting up a fake website or compromising a legitimate one in order to exploit visiting users;
- **ransomware** - which could include disseminating disk encrypting extortion malware; and
- **scanning** - attacking wide swathes of the Internet at random.

4.9 In targeted cyber-attacks, an organisation is singled out because the attacker has a specific interest in the business or has been paid to target the organisation. A targeted attack is often more damaging than an un-targeted one because it has been specifically tailored to attack systems, processes, or personnel, in the office and sometimes at home. Targeted attacks may include:

- **spear-phishing -** sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software;
- **deploying a botnet -** to deliver a DDOS (Distributed Denial of Service) attack; and
- **subverting the supply chain** - to attack equipment or software being delivered to the organisation.

5.0 The Local Government Association (LGA) recognises that in recent years there has been a significant rise in cyber security related incidents affecting the public sector across the globe, as well as a marked increase in the number of attacks targeting national infrastructure, such as healthcare, local government and even water supplies. Not only are these incidents becoming more frequent, but they are also becoming increasingly sophisticated and appear to be carried out by advanced, persistent threat actors that have access to considerable resources. As a response to this, it is vital for authorities to ensure they have the knowledge, means and support to effectively defend themselves against determined adversaries and relentless cyber-attacks.

5. MAIN FINDINGS

5.1 Obj1: Policy and Procedures

5.1.1 The 5CP/Capita have 14 IT cyber security policies and procedural documents, which have been agreed and implemented through the partnership. These polices are not specific to South and Vale operations, and due to this complexity, the policies and procedures are not issued to officers. The IT manager is developing an IT security policy, specific to South and Vale operations, which amalgamates all 14 5CP policies into one operational document. Aa of September 2022, the policy is in draft, awaiting senior management team (SMT) sign-off.

5.1.2 The annual review of 11 out of the 14 5CP/Capita polices are overdue. The policies are being reviewed and updated within the 5CP security working group; however, not all policies have been approved and published.

5.1.3 During the previous internal audit in 2019/20 the organisation had not developed their own cyber security strategy, due to other priorities. This was

still the case at the time of this review (September 2022). 5CP/Capita have a cyber incident response procedure from a technical service perspective; however, there is no localised plan that covers internal council operations. The assurance team are developing a South and Vale cyber response incident plan, which has not been finalised.

5.1.4 The councils have embedded a variety of controls to mitigate the occurrence of a cyber security breach, as documented in the draft joint IT security policy. Controls include requirements for passwords, email usage, internet and wireless networks, virus checking software, screen savers, the storage of business data, system updates, confidentiality, confidential media, remote access, mobile telephony, security incidents, business continuity, and IT systems monitoring.

5.1.5 In November 2021, South and Vale launched multi-factor authentication (MFA) to provide an extra layer of protection to council systems, which has improved cyber security for staff, council members, and the organisation.

5.1.6 The councils have in place their own joiner/mover/leaver (JML) process with Capita, where authorised individuals (usually service manager level and above) may approve requests for changes to IT systems and account access by submitting the relevant form to the Capita service desk. A copy of the agreed JML policy/procedures could not be provided during the review; however, a copy was provided by Capita following the internal audit exit meeting. The 5Cs JML procedure does not reflect the South and Vale approval process in place; however, controls within this area are due to be reviewed.

5.1.7 Weaknesses were identified within the sample testing of the current JML process. The Capita service desk had not updated the councils' approved personnel list and were found to be using an historic (outdated) version. Furthermore, our results identified anomalies within 18 (60%) of the 30 requests sampled, where ten (33%) request forms were approved by individuals not listed on the appropriate authorisation list for the period and eight (26%) were not supported with a physical request form on file (requests had been submitted directly via email or phone call to the service desk). Additionally, none of the 'mover' change requests submitted to Capita following a role change or movement to another service within the councils' evidenced requests for prior access to be revoked (mailboxes/systems/shared folders), but focused on approving additional access permissions, which may impact data protection and information governance requirements.

5.1.8 Area assurance: Limited
Four recommendations have been made as a result of our work in this area (Recs 1 to 4).

5.2 Obj2: Training and guidance

5.2.1 A cyber security training module (stay safe online) is available on the online learning management system, Learning, Education and Achievement Hub (LEAH) and has been developed with guidance and information from the National Cyber Security Centre (NCSC). The module forms part of the mandatory induction training for new starters to complete during the six-month probation period. The course has been available on LEAH since December

2020, and it is the individual service manager's responsibility to monitor their team's completion through the HR probation review process.

5.2.2 As at July 2022, 56 officers across had completed the mandatory online training module since December 2020. Based on a total of 540 (356 South and 184 Vale) employees (July 2022), this represents a 10% completion rate.

5.2.3 Agency staff and contractors working on behalf of the councils are not required to complete the mandatory training, as they are not directly employed by the councils and fall outside of the HR onboarding process. The councils do not keep a record of the number of agency/temporary hires made; however, based on a recent Freedom of Information (FOI) request, South and Vale paid a total of £2,457,897 (South £1,999,216 and Vale £458,681) for temporary agency staff for the period (1 April 2021 to 31 March 2022), including recruitment costs.

5.2.4 Review found that of the 32 new starters in the sample period (September 2021 to December 2021), 16 (50%) were casual staff who would not necessarily be required to complete the mandatory training due to holding positions with limited systems access (café assistants, elections canvassers and Beacon duty officers). Of the remaining 16 individuals, two (12%) had completed the mandatory module within the required six month period and 14 (88%) had not completed the mandatory training module, and were still employed by the councils.

5.2.5 The HR Advisory team are developing a new employee induction programme which is due to be launched in November 2022. Although the mandatory cyber security module forms part of a new starter's induction programme, it does not require new starters to read the IT Security Policy. Additional training materials have been purchased through MetaCompliance to strengthen the information and cyber security training provided to officers. The IT Manager is working with the HR Advisory team to add the training materials in LEAH.

5.2.6 Information and cyber security training was last provided to councillors in June 2020, following the 2019 council elections. No further training has been delivered since this initial training session; however, a new councillor cyber and data security presentation is being developed by the assurance team, with assistance from the IT manager, which will be shared with members after the elections in May 2023. There are information and cyber security pages on Jarvis specifically for councillors, which provide information on home working, passwords complexities, scam awareness, ransomware, and the dangers of public Wi-Fi. It also has information on how to access the council network through the VPN and using MFA. The member newsletter, InFocus, is another source of information (e.g., IT updates, cyber security reminders).

5.2.7 The Jarvis 'Be Cyber Secure' information page promotes the importance of cyber security to protect the councils' IT equipment and safeguard against data leaks and financial loss. This page provides officers details on workstation security, passwords complexity, scam awareness, ransomware, and the dangers of public Wi-Fi. The guidance also advises officers what to do if they suspect their internet security has been breached, with contact and escalation details, and signposts officers to the relevant cyber security training available on LEAH. A link is also present on this page directing officers to the

'Managing Information' page, which gives further, specific information, on the management of records and data protection.

5.2.8 Following the adoption of flexible working arrangements, further guidance has been published relating to home and remote working. The guidance includes IT security and best practices for officers utilising communication apps, including Microsoft Teams, WhatsApp and Zoom and provides detailed information to support officers conduct their duties securely from a remote location (non-council building). We identified a conflicting statement within the guidance regarding Wi-Fi connection access, which needs review.

5.2.9 The cyber and data security group (made up of officers from IT, assurance, information governance and communications) have implemented quarterly 'communication takeovers' to promote and remind officers and members of their responsibilities surrounding information and cyber security. This involves various 'hot topics' being communicated via an email outburst to all employees. These outbursts are generally targeted around holiday seasons to reiterate the councils' message on data and information security over this period. Topics have included, general security guidance, password complexities and staying cyber safe. This channel is also used to issue reactive communications and directions for incident management following any potential information security risk being identified, whether directly by the councils, or through the extended 5CP security working group.

5.2.10 Area assurance: Limited
Three recommendations have been made as a result of our work in this area (Recs 5 to 7).

5.3 Obj3: Information and security breach reporting

5.3.1 The 5CP have an agreed cyber security response and incident management policy, last reviewed in August 2020. This is supported by the 5CP cyber incident response procedure (last reviewed July 2022), which details the process and procedures to be followed by Capita IT staff and 5CP officers (including members who form the joint 5CP security working group) in response to a cyber security incident.

5.3.2 Both documents detail the agreed reporting process and incident management route, including identification, detection and analysis, containment, eradication, recovery, and incident closure. The different types of cyber/information security incidents are also categorised and graded through a triage matrix with a stepped incident response plan for each priority level. A priority 1 incident is categorised as distributed denial-of-service (DDoS) attack against the 5CP network, attacks against network infrastructure, network disruption for a large segment of council users, ransomware/criminal activity, and destructive malware. For each priority 1 (P1) major incident, a post incident report (PIR) is required to be completed by Capita and issued to all implicated parties including a summary of the incident management response and lessons learned.

5.3.3 South and Vale have been impacted by one priority 1 (P1) security incident since April 2022. In June 2022, Capita were informed of a P1 phishing incident across the 5CP that impacted both South and Vale users (a phishing email purporting to be from Dorset council was opened by 29 users across

the 5CP). A copy of PIR is outstanding; however, there is no agreed timescale for reports to be provided to affected parties and a verbal recommendation has been raised. Following the reporting of a cyber/information security incident, the councils' information governance team now includes details of all incidents onto the council's data breaches and security incident log, to assist identifying any potential trends or weaknesses in local (council owned) process and procedures.

5.3.4 The Jarvis 'Be Cyber Secure' information page states what officers are required to do in the event of a suspected cyber security breach. This includes the appropriate reporting route and contact details. A similar page is published for councillors.

5.3.5 The cyber and data security group meets monthly (via Teams) to discuss current and emerging cyber and data risks across South and Vale and those shared between the 5CP to ensure there are suitable controls in place to protect the organisation.

5.3.6 South and Vale form part of the external 5CP IT Security Working Group, which meets monthly. Representatives from IT, assurance and information governance teams represent South and Vale, with similar representation from the five councils and Capita. During the meetings, Capita shares performance metrics relating to information security and data incidents, encryption, anti-virus updates on devices, patching, devices not rebooted, malware and phishing summaries, spam detections and spoof email interceptions.

5.3.7 Area assurance: Full
One verbal recommendation has been made as a result of our work in this area.

5.4 **Obj4: Risk management**

5.4.1 South and Vale have their own corporate risk registers, which are maintained by the assurance team. The latest risk registers were presented to the Joint Audit and Governance Committee (JAGC) on 5 July 2022. Both risk registers have four medium to high risks in relation to information and cyber security controls, including the highest risk facing both councils, in relation to third party business continuity and disaster recovery routines (see objective 5).

5.4.2 The corporate risk registers are routinely reviewed (at least every six months) and shared with SMT prior to being presented to members at JAGC. Within the corporate risk registers mitigations and planned actions are also documented against each IT security risk. The corporate risk registers acknowledge and recognise several cyber threats and risks to information security breaches and malicious attacks.

5.4.3 Individual service team risk registers (29 in total) are available on Jarvis and are reviewed and updated on a quarterly basis. A named officer (risk champion) for each service team is allocated the responsibility to review and update the register. This is then submitted to the assurance team to review and publish on Jarvis.

5.4.4 We reviewed a sample of 16 (55%) service team risk registers to confirm whether information and cyber security risks is identified and acknowledged.

Only eight (50%) risk registers contained cyber/information security related risks and mitigations, including included six services perceived at a higher risk due to their involvement/access to operating systems, financial systems, accounts, and/or sensitive personal data. In addition, 14 (88%) of the 16 risk registers are overdue for review. Furthermore, high level risks identified in the corporate risk registers are not consistently cascaded through to the service team risk registers, to ensure that operational controls are in place.

5.4.5 In June 2021, both South and Vale were selected to undergo a cyber security penetration test by the Local Government Association (LGA). The test was conducted on behalf of the LGA, by Dionach. The test identified several critical and high-risk issues, in addition to lower risk issues identified in all areas of the assessment. The councils were issued with a joint action plan suggesting recommendations to address the issues raised. Overall, 48 recommendations were raised (five critical, 11 high risk, 15 medium risk, and 17 low risk). The recommendations have been reviewed and are now outdated, as some areas have changed across the estate since the test date. The LGA report was passed to Capita, as service providers, to review and provide response. Capita are now conducting their own annual penetration tests and it is planned that the findings of from the 2021 and 2022 tests will include responses to the LGA report; however, the status of progress against these recommendations was unclear.

5.4.6 The assurance team are exploring options for taking out additional insurance policies for both South and Vale relating to cyber security attacks and information security breaches. Due to pandemic, and subsequent flexible working practices, there is a greater risk of information and cyber security breaches. Consequently, the assurance team decided to revisit the insurance policies to determine whether there is now a requirement to expand coverage based on the councils' risk rating. The assurance team have instructed the insurance broker to begin the cyber risk evaluation process, to understand whether additional policy coverage is needed.

5.4.7 Area assurance: Limited
Three recommendations have been made as a result of our work in this area (Recs 8, 9 and one verbal recommendation).

5.5 Obj5: Disaster recovery and business continuity

5.5.1 As reported in the 2019/20 audit, there is no corporate (council owned) disaster recovery plan (DRP) in the event of a cyber/information security incident across council systems. Capita have a generic disaster recovery plan to cover their systems; however, as previously noted, this plan was rejected by both South and Vale as it is not specific to the organisation and does not meet the councils' requirements. Since 2019/20, IT system management has progressed, with more IT applications being hosted on cloud-based servers and individual disaster recovery agreements in place with providers. Capita have also introduced annual disaster recovery testing routines for Capita hosted non-cloud systems (see 5.5.2 below). The requirement for a council owned DRP is mitigated, on the basis that suitable Business Continuity Plans (BCP) are in place.

5.5.2 Capita conduct annual disaster recovery (failover) testing across selected 5CP systems. Testing was completed for the South and Vale GIS system in

June 2021: testing was successful, and no critical issues were identified. Testing in 2022 was conducted in July and the councils selected the ModGov (democratic services) system. Testing was successful; however, an unforeseen issue relating to database access resulted in calls to the IT helpdesk. It is anticipated that this issue will be documented on the lessons learned section of the Capita report, once received.

5.5.3 The Jarvis business continuity page advises that the councils are in the process of updating the business continuity strategy and in the event of an emergency in the districts, officers will require access to certain documentation (e.g., crisis management plan, setting up calls in an emergency). The documentation was last published in 2013 and a review is needed to confirm they still align to applicable legislation and the councils' delivery of services and systems. The planned review of this area was put on hold due to the pandemic and diversion resources to other priorities.

5.5.4 Each service team has a business resilience plan (BRP) detailing its live status against challenges in delivering their services and work is underway to update plans with service teams. It is recommended that the business resilience plans (BRP) are acknowledged within an overarching corporate business continuity plan (BCP) to ensure that a consistent approach is taken in the event of a major systems failure. In addition, in the 5CP cyber incident response procedure, there is no acknowledgement of cyber and information security incidents that may occur 'out of hours', or over a long public holiday, such as the councils' extended Christmas office closure, where there may be limited access to the councils' DPO, SIRO and IT manager.

5.5.5 Capita have 30 days of backups at any one time; however, there is no cold store (offline) backup of council data. All backups are completed as cloud based (online) routines, as such, are more susceptible to potential major ransomware and malware cyber-attacks. There is a planned project underway to review the separation of South and Vale from Microsoft Office 365 applications, security controls and back-ups, and to move the council's IT application servers to a cloud-based service (Microsoft Azure), giving the councils more control in relation to the management of these applications. The 5CP security working group has asked Capita to provide a suitable offline (cold store) backup solution for remaining servers hosted within the Nuvem platform, until these are transitioned to Azure, expected in Q1 2023.

5.5.6 Area assurance: Limited
Two recommendations have been made as a result of our work in this area (Recs 10 and 11).

6. ACKNOWLEDGEMENTS

6.1 Internal audit would like to take this opportunity to thank all staff involved for their assistance with the audit.

RECOMMENDATIONS

Obj1: Policy and procedures 1. IT Security Policy and Procedures		Risk Rating: High Risk Score: 8
Findings	**Recommended Action(s)**	**Action Owner(s)**
Findings Capita/5CP have14 IT cyber security policies and procedures, agreed and implemented through the 5CP partnership, that are not specific to South and Vale operations. As a result, these are not published to South and Vale council officers. A policy is being developed that amalgamates all 5CP policies into one operational document specific to South and Vale operations; however, at the time of review (September 2022) this was in draft and had not been signed off by the senior management team. Support resources are available through the Local Government Association (LGA) for a variety of IT and Cyber Security practices – highlighting good practice that councils can employ to improve their cyber security posture and practices. We recommend that this framework is considered in the development of South and Vale IT policies and procedures. Risk(s) Without an adequate IT security policy and procedures there is a risk that officers may not be aware of the requirements surrounding IT and cyber security practices. Officers may lack awareness of their individual responsibilities and requirements to information and cyber security, which may increase the risk of a network breach.	Finalise and publish an IT security policy and associated procedures to officers and members, that aligns to the councils' IT operations, LGA framework, and relevant legislation.	IT Programmes Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Draft policy has been through approval stages but needs review before agreement and adoption Management response: IT Programmes Manager		31 March 2023

Obj1: Policy and procedures 2. Joiners, Movers, and Leavers (JML)		Risk Rating: High Risk Score: 8
Findings	**Recommended Action(s)**	**Action Owner(s)**
The process to request changes to systems access requires a form to be completed and sent to the Capita IT Helpdesk which is then cross-referenced to an approval list provided to the Capita service desk team, by the council's IT Manager. A copy of the agreed JML policy/procedures could not be provided during the review; however, a copy was provided by Capita following our exit meeting. From our review of the 5Cs Joiners, Movers and Leavers Process (JML) Procedure, it does not reflect the South and Vale approval process in place. We were advised that controls within this area are due to be reviewed. It is noted during our review that the Capita service desk team were utilising an outdated, historic version of the authorised approvers document, that listed some individuals who were no longer employed by the councils. Internal audit randomly selected a sample of ten change requests for each area of the process, new starter (Joiner), mover and leaver (30 tests in total) for both South and Vale based employees, over the period April to June 2021. Our results identified anomalies within 18 (60%) of the sample reviewed where ten (33%) request forms were approved by individuals not listed on the appropriate authorisation list for the period and eight (26%) were not supported with a request form on file (requests had been submitted directly via email or phone call to the service desk). Additionally, none of the change requests submitted to Capita following a role change or movement to another service within the councils' (mover) evidenced requests for prior access to be revoked (mailboxes/systems/shared folders), but focused on approving additional access permissions. <u>Risk(s)</u> Without a defined JML policy and process in place there is a risk that system approvals may be granted to individuals who are not authorised to submit requests. Access to systems, accounts and sensitive data may be obtained surreptitiously for personal gain by unauthorised persons. Individuals may be granted access to systems and files that are not appropriate for their role, including persons who leave the councils that may still have access rights enabled.	a) Review, agree and formalise the South and Vale JML policy, procedures, and associated documentation (including defined procedures for management of the active directory) and publish updated guidance to officers and the Capita service desk. b) Capita service desk to remind officers that only requests signed/submitted by individuals listed on the agreed (current) JML approvals register may authorise changes to IT systems and accounts.	Capita Head of IT Services & Capita Information Security Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** JML documentation shared along the return of this form and Capita will undertake a review of the findings to ensure process is followed and draw out any alternative steps taken to seek approval in the absence of hiring manager etc. Management response: Capita Head of IT Services		31 December 2022

Obj1: Policy and procedures 3. Cyber security response strategy/plan (*restated*)		Risk Rating: Medium Risk Score: 5
Findings	**Recommended Action(s)**	**Action Owner(s)**
5CP/Capita have in place a Cyber Incident Response Procedure from a technical service perspective, however, there is no localised plan that covers internal council operations. During the last audit (2019/20) the councils had not developed their own cyber security strategy, due to other priorities. Internal audit established a Cyber Response Incident Plan is being developed for South and Vale. At the time of review (September 2022), this was in draft and had not been finalised. <u>Risk(s)</u> If a cyber security response strategy is not in place, there is a greater risk of cyber security incidents not being managed appropriately resulting in possible breaches to the councils' network, systems, and sensitive data.	a) Finalise a cyber security response strategy/plan and obtain approval in line with the councils' Constitution. b) Communicate the cyber security response strategy with council officers, members, and Capita IT.	Assurance team leader, Emergency Planning Officer, Programmes and Assurance Manager, & IT Programmes Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** a) A draft Cyber incident response has been developed and will be incorporated into the councils Emergency Plan Protocols as an example of a type of emergency BC scenario. The proposed approach will be reviewed and agreed by SMT, Capita IT and IT Programmes Manager officers and members. This is further supported by the councils' Business Continuity Plan approach. Staff awareness to be incorporated as part of ongoing Cyber awareness seasonal campaigns through Communications. b) Once the plans are finalised communication of the plans will be distributed to those listed through usual channels. Management response: Assurance Team Leader/Emergency Planning Officer/IT Programmes Manager		31 March 2023

Obj1: Policy and procedures		Risk Rating: Low
4. 5CP/Capita Security Policy and Procedures		Risk Score: 3
Findings	**Recommended Action(s)**	**Action Owner(s)**
Capita/5CP currently have in place 14 IT/cyber security policies and procedural documents that have been agreed and implemented through the 5CP partnership. These polices state an annual review will be conducted. Per our review of records provided, it is noted that the annual review for all policies is overdue, and 11 policies have not been reviewed since 2020. Several policies contain outdated contact information for South and Vale service teams. The Interim Executive IT Client (5CP) advised that these policies are currently being updated and new versions should be available by the end of August/September 2022. Following an update during the exit meeting, internal audit was informed that the review has progressed, however, not all polices had been approved/published operationally at the time of writing this report. <u>Risk(s)</u> Without regular review, polices may become outdated and contain inaccurate procedural information that may impact an effective response following an incident.	The 5CP security working group to review and approve all owned IT policies to ensure the information contained within remains relevant and accurate to individual 5CP services.	Capita Information Security Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Ensure all Information security policies are updated, and version controlled following the feedback received from the 5Cs DPOs. All Information Security policies have been reviewed and evidence supplied to the Council. Management response: Capita Information Security Manager		Implemented between draft and final report stage

Obj2: Training and guidance		Risk Rating: High Risk Score: 8
5. Training (council employees, agency staff, contractors, and members)		
Findings	**Recommended Action(s)**	**Action Owner(s)**
Officers are required to complete 'Stay Safe Online (Top Tips for Staff)', mandatory cyber online training module on LEAH within their probation period (usually within six months of their start date). There is no requirement in place for information/cyber security refresher training to be completed. From our review of system reports: • In total there were 56 officers across both South and Vale that had completed the mandatory online training module since it launched in December 2020. Based on current employee numbers, (as of July 2022), this represents 10% of officers employed across both councils, (356 South and 184 for Vale). • Review also showed that of the 16 new starters eligible to complete the training, two (12%) had completed the mandatory module within the required six month probationary period, and 14 (88%) had not completed (or started) the mandatory training. Through enquiries, internal audit was advised that there is currently no requirement for agency staff and contractors working on behalf of the council to complete the mandatory information and cyber security training, as they do not form part of the HR onboarding process (not registered on the payroll establishment list and LEAH training system); however, still access the same council systems as permanent employees to conduct their duties. Cyber security training was last provided to Councillors following the council elections in June 2019. No further training has been conducted since this initial training session was delivered. A new Councillor Cyber and Data Security presentation is being developed by the assurance team, with the assistance of the IT Manager, with a view to present and publish the presentation to members on conclusion of the 2023 elections. <u>Risk(s)</u> Individuals accessing council systems are unaware or have not completed the council's information/cyber security training resulting in a lack of understanding of key risks and practices that should be followed to mitigate the occurrence of cyber and information security incidents.	a) Issue service managers a regular LEAH training compliance report to assist monitoring completion of mandatory training. b) Review requirements for agency staff, contractors, and members to complete mandatory information/cyber security training to ensure awareness of council IT security practices. c) Finalise, present, and publish the revised Cyber and Data Security presentation to all members. d) A regular schedule for information/cyber security refresher training to be established.	IT Programmes Manager & People and Culture Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Updated cyber security training is being installed onto LEAH which is more focused on specific themes. Management response: IT Programmes Manager, People & Culture Manager		a) 31 March 2023 (once new induction programme has been rolled out) b) 31 December 2022 c) Following elections on 4 May 2023 d) 31 March 2023 (once training programme is completed and released onto LEAH)

Obj2: Training and guidance 6. Guidance records		Risk Rating: Medium Risk Score: 5
Findings	**Recommended Action(s)**	**Action Owner(s)**
Various guidance documents relating to information and cyber security is published to officers and members on the council's intranet, Jarvis. Within a supporting guide titled 'Remote working IT guide for officers & Councillors', it is noted that the point relating to Wi-Fi connections does not clearly state that the use of public Wi-Fi is not permitted and should be clarified. Guidance states: 'If you are within the council office your device will connect automatically to the council's Wi-Fi network. Outside the offices you can use any Wi-Fi network to which you have access, but you must use the VPN to secure the connection'. This contradicts the general cyber security guidance published on Jarvis that states that public Wi-Fi cannot be used due to the network being insecure. Additionally, it is noted that the contact details for the council's named DPO and service manager require updating within the 'essential guides' documentation (previous service team and DPO listed). <u>Risk(s)</u> Without clear and accurate guidance officers may not be aware of information and cyber security controls and practices that should be followed to mitigate the occurrence of cyber and information security incidents.	Review and update supporting information and cyber security guidance published on Jarvis, including the 'Remote working IT guide for officers & Councillors' to ensure accuracy in operational practices and contact details.	IT Programmes Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Guidance documentation will be updated to provide accurate information on operational practices for officers and members of the councils Management response: IT Programmes Manager		30 November 2022

Obj2: Training and guidance 7. Employee induction programme		Risk Rating: Low Risk Score: 3
Findings	**Recommended Action(s)**	**Action Owner(s)**
The HR Advisory team are developing a new employee induction programme that lists a number of mandatory training modules and council polices that are required to be reviewed/completed by new starters during their probation period. The draft document does not list the council's IT Security Policy as a requirement and should be considered. <u>Risk(s)</u> Officers are unaware of the council's IT Security Policy resulting in a lack of understanding of key risks and practices that should be followed to mitigate the occurrence of cyber and information security incidents.	Following implementation of the council's IT security policy, the IT Manager to notify the HR Advisory team to update the employee induction document to include a requirement to confirm individuals have read the councils' IT security policy.	IT Programmes Manager & People and Culture Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** IT Programmes team to agree with People & Culture on requiring the IT Security Policy to be part of inductions programmes. Management response: IT Programmes Manager		31 March 2023 (once the policy is implemented)

Obj4: Risk management 8. LGA audit recommendations		Risk Rating: High Risk Score: 8
Findings	**Recommended Action(s)**	**Action Owner(s)**
In June 2021, both South and Vale were selected to undergo a cyber security penetration test by the Local Government Association (LGA). The test was conducted on behalf of the LGA by Dionach. The penetration test revealed three high risk issues for the external network assessment, two high risk issues for the web application assessment, and five critical and six high risk issues for the internal network assessment. In addition, lower risk issues were identified in all areas of the assessment. The councils were issued with a joint action plan suggesting recommendations to address the issues raised. Overall, there are 48 recommendations listed, five rated critical, 11 high risk, 15 medium risk and 17 low risk. The IT Manager advised internal audit that the recommendations have been reviewed and are now fairly out of date, as some things have changed across the estate since the testing was initially completed. The LGA report was passed to Capita, as service providers, to review and provide response. Capita are now conducting their own annual penetration tests and it is planned that the findings of 2021 and 2022 test results, include responses to the LGA report; however, the current status of progress against these recommendations was unclear. <u>Risk(s)</u> Where recommendations are not addressed, the councils remain exposed to unmitigated risks.	Review and address the outstanding recommendations within the LGA/Dionach cyber security penetration test report where risks remain relevant.	Capita Information Security Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Capita to instigate a SIP to accelerate the closure of all remaining vulnerabilities. Management response: Capita Information Security Manager		31 December 2022

Obj4: Risk management 9. Risk registers (Services)		Risk Rating: Medium Risk Score: 5
Findings	**Recommended Action(s)**	**Action Owner(s)**
The councils' corporate risk registers identify the following IT information/cyber security risk: • IT and data security compromised due to remote working and naive user behaviour, which may result in data breach and fines/loss of reputation. Individual service team risk registers (29 in total) are available on Jarvis. The registers are reviewed and updated on a quarterly basis, with the most recent register being published. Internal audit selected a sample of 16 (55%) risk registers to ascertain whether information and cyber security risks had been identified and acknowledged within the service registers. Review of the 16 risk registers found eight (50%) contained cyber/information security related risks and mitigations and eight (50%) did not. This included the following six services perceived at a higher risk due to their involvement/access to operating systems, financial systems, accounts, and/or sensitive personal data: 1. Finance, Revs and Bens and Strategic Finance, Internal Audit, Exchequer and Procurement; 2. People and Culture; 3. Customer Services; 4. Community Hub and Recovery; 5. Legal and Democratic Services; and 6. Strategic IT. In addition, 14 (88%) risk registers are overdue for review, the oldest dated as last reviewed in February 2021, and eight (50%) have not been reviewed in the last 12 months. <u>Risk(s)</u> Service teams may not identify information and cyber security risks associated to their operations, which may result in inadequate controls to mitigate targeted network breaches. If risk registers are not regularly reviewed, there is a risk that evolving corporate risks may not be identified and suitable controls implemented at operational level to protect the service and organisation.	a) The assurance team to work with the service risk champions to ensure that cyber and information security corporate risks and controls are suitably cascaded to operational level. b) A process to be implemented to ensure that service team risk registers are reviewed and kept up to date on a quarterly basis, in line with the published guidance on Jarvis.	Assurance Team Leader & Programmes and Assurance Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Amendments to the risk management framework are being developed at the moment and this issue will be incorporated into the process. In the meantime all risk champions will be asked to review their service risk registers to incorporate a cyber and data security risk. The corporate and service risk registers will be updated following the risk management framework review and will incorporate any new risks identified prior to the next report to JAGC in 2023. Management response: Assurance team leader		31 July 2023

Obj5: Disaster recovery and business continuity 10. Business continuity plan		Risk Rating: High Risk Score: 8
Findings	**Recommended Action(s)**	**Action Owner(s)**
There is a dedicated business continuity page published on the council's intranet, Jarvis, that advises that the councils are in the process of updating the business continuity strategy. It is noted that these documents were last reviewed/published in 2013 and a review is overdue. The councils previously had in place a Corporate Business Continuity Plan (BCP); however, this document was also last updated in 2013 and requires review to ensure it aligns to relevant legislation and the council's current delivery of services and systems. Planned review of this area was put on hold due to the Covid-19 pandemic and resource applied to assist the delivery of key council services through the period. Each service team has in place a Business Resilience Plan (BRP) that details the live status against challenges of delivering their services. Internal audit was advised that a review is underway to update these documents with each service team. At the time of review (September 2022) progress was ongoing, however, not all information had been returned/updated by individual service teams upon review. Additionally, per our review of the Five Councils Partnership Cyber Incident Response Procedure, there appears to be no acknowledgement to cyber and information security incidents that may occur 'out of hours', or over a long public holiday, such as the council's extended Christmas office closure, where there may be limited access to the council's DPO, SIRO and IT Manager. Suitable considerations should be given to ensure cyber and information security incident management can operate appropriately during 'out of hours' periods and ensure business continuity. <u>Risk(s)</u> Failing to address disruption that impacts on business continuity may result in reduced productivity (staff can't access systems), financial loss (payments and fees are unable to be processed), reputational damage (trust in an organisations procedures may be questioned) and business failure (unable to provide services).	a) Review, update and publish the corporate business continuity strategy/plan in preparedness for a cyber/information security incident ensuring the plan provides suitable coverage for incidents that may occur 'out of hours' b) Once a revised business continuity strategy/plan is in place, undertake a regular review to ensure that the plan is fit for purpose.	Assurance Team Leader, Emergency Planning Officer, Information Governance Officer & IT Programme Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Capita have a joint BC/DR plan that has been adopted and the DR elements of this have been tested in 2022. As part of the councils business continuity arrangements we will review and update the IT Corporate Business Continuity prioritisation and ensure that this is incorporated into our service business resilience plans. This will enable us to derive an approach based upon priority activities across all service teams. Regular Capita DR testing to be agreed in collaboration with IT systems manager. Service BRP Template under revision which will include a standard line linking to the IT DRP. A scenario to be set to incorporate a cyber/data incident out of hours in the BRP's as an exercise across the council using the DRP, linking to BRP's. Management response: Assurance team leader/ Information Governance Officer/IT Programme Manager		31 July 2023

Obj5: Disaster recovery and business continuity		Risk Rating: High
11. Back up routines		**Risk Score: 8**
Findings	**Recommended Action(s)**	**Action Owner(s)**
There is no cold store (offline) backup of council data. All backups are completed as cloud based (online) routines, as such, are more susceptible to potential major ransomware and malware cyber-attacks. The IT Manager confirmed that Capita have 30 days of back up at any one time. Internal audit was advised that there is a planned project underway to review the management of Office 365 applications, security controls and back-ups, and to move the council's IT application servers to a cloud-based service (Microsoft Azure). The Interim Executive IT Client (5CP) confirmed that Capita have been asked to revisit the potential for an offline (cold store) backup solution for all servers hosted in the Capita Nuvem platform. <u>Risk(s)</u> Without an offline (cold store) backup there is no way of accurately restoring data following a ransomware attack.	Capita to provide a suitable offline immutable backup solution for servers hosted within the Capita provided platforms (e.g. Nuvem, Azure), currently being pursued by the 5CP security working group.	Capita Head of IT Services
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Proposal for offline backup submitted to PM/5CL's 02/11. Awaiting councils' response on whether to proceed. Management response: Capita Head of IT Services		30 November 2022 Subsequent activity is dependent upon council response.

APPENDIX 1 – CATEGORISATION OF RECOMMENDATIONS

1.1 Audit recommendations have been assigned a risk rating, based on the below 3x3 risk matrix. The risks identified in each recommendation are examined to determine:

- the impact the risk would have against achieving the objective; and
- the likelihood that the event will occur

3x3 RISK MATRIX				
IMPACT	Critical (>10%)	6	8	9
	Major (2-10%)	2/3	5	7
	Manageable (<2%)	1	2/3	4
		Remote (<10%)	Possible (10-50%)	Likely (>50%)
		LIKELIHOOD		

1.2 To assist management in using our reports, we have categorised our recommendations, in line with the 3x3 risk matrix, according to their level of priority as follows:

Risk rating	3x3 risk score	Recommendation(s)
High risk	7-9	Recs 1, 2, 5, 8, 10 and 11
Medium risk	4-6	Recs 3, 6 and 9
Low risk	2-3	Recs 4 and 7
Very low risk	1	Two verbal recommendations were raised during audit fieldwork

APPENDIX 2 - AUDIT FRAMEWORK

1. AUDIT OBJECTIVES

1.1 The audit was designed to ensure that management have implemented adequate and effective controls over information (inc. cyber) security.

1.2 Internal audits are undertaken in accordance with a priority score stated within the schedule of auditable activity, and following an initial assessment by internal audit, external audit and the councils' section 151 officer.

1.3 Drivers for audit reviews include:

- date last reviewed;
- last assurance rating;
- exposure to financial risk;
- exposure to fraud risk;
- exposure to reputational risk;
- exposure to legal risk;
- exposure to corporate risk; and
- whether an officer has requested a review.

2. AUDIT APPROACH AND METHODOLOGY

2.1 The audit approach was developed with reference to the internal audit charter and by an assessment of risk and management controls operating within each area of the scope.

2.2 The aim of an audit is to establish if:

- there are adequate internal controls in effective and efficient operation;
- the processes are meeting the requirements of internal policy and procedural standards; and
- the processes are meeting external codes of practice, professional and statutory regulations.

2.3 The following procedures were adopted:

- identification of the role and objectives of each area;
- identification of risks within the systems and controls in existence to allow the control objectives to be achieved; and
- evaluation and testing of controls within the systems.

From these procedures we have identified weaknesses in the systems of control, produced specific proposals to improve the control environment and have drawn an overall conclusion on the design and operation of the system.

APPENDIX 3 - STAFF INTERVIEWED AND REPORT DISTRIBUTION

1. STAFF INTERVIEWED

1.1
- Simon Turner, IT Manager
- Paul Merrick, Interim Executive IT Client (5CP)
- Tassadaq Hussain, IT Security Manager (Capita)
- Ian Thompson, Infrastructure Team Lead (Capita)
- Allison Holliday, Risk and Insurance Officer
- Gary Carey, Emergency Planning and Business Continuity Officer
- Yvonne Cutler-Greaves, Assurance Team Leader
- Sandy Bayley, Information Governance and Data Protection Officer
- Steve Culliford, Democratic Services Team Leader
- Steven Corrigan, Democratic Services Manager
- Abigail Lee, HR Co-ordinator
- Louis Raymond, Strategic HR Coordinator
- Jaydon Perrin, HR Advisor
- Trina Mayling, Strategic HR Business Partner
- Ben Coleman, Programmes and Assurance Manager

2. REPORT DISTRIBUTION

2.1 A copy of this final report has been distributed to the following officers:

- Paul Merrick, Interim Executive IT Client (5CP)
- Tassadaq Hussain, Information Security Manager (Capita)
- Parul Patel, Interim Head of IT Service 5CL's (Capita)
- Yvonne Cutler-Greaves, Assurance Team Leader
- Trina Mayling, Strategic HR Business Partner
- Sandy Bayley, Information Governance and Data Protection Officer
- Simon Turner, IT Manager
- Ben Coleman, Programmes and Assurance Manager
- David Fairall, People and Culture Manager
- Mark Minion, Head of Corporate Services
- Harry Barrington-Mountford, Head of Policy and Programmes
- Patrick Arran, Head of Legal & Democratic (Monitoring Officer, DPO, SIRO)
- Simon Hewings, Head of Finance (S151 Officer)
- Adrianna Partridge, Deputy Chief Executive
- Mark Stone, Chief Executive
- Cllr Andrea Powell, South Portfolio Holder
- Cllr Debby Hallett, Vale Portfolio Holder

STATEMENT OF RESPONSIBILITY

Internal audit takes responsibility for this report, which is prepared on the basis of the limitations set out below.

INTERNAL AUDIT NOVEMBER 2022

Contact Persons:

John Tredrea	**Auditor** **Mob: 07598 553016** **Email: john.tredrea@southandVale.gov.uk**
Victoria Dorman-Smith	**Internal Audit Manager** **Mob: 07766 780835** **Email: victoria.dorman-smith@southandVale.gov.uk**

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work should not be taken as a substitute for management's responsibilities for the application of sound practices. We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses that may exist. Nor should internal audit work be relied upon to identify all circumstances of fraud or irregularity should there be any, although our audit procedures have been designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of internal control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance. Effective implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

This report has been prepared solely for SOUTH and VALE use. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose.