STAFFORDSHIRE FIRE AND RESCUE SERVICE

Cyber Risk Assessment (CRA)

Final Internal audit report 6.22/23

3 May 2023

1. EXECUTIVE SUMMARY

Why we completed this audit

An audit of Cyber Risk Assessment was undertaken at Staffordshire Fire and Rescue Services ('Staffordshire', 'the service') as part of the approved internal audit plan for 2022/23. The objective of the review was to perform an independent assessment of the current level of cyber risk protection, awareness, and good practice, confirming that computer systems and data are resilient to internal and external cyber threats. Cyber risk has been defined by the Institute of Risk Management (IRM), as any risk of financial loss, systems disruption, or damage to the reputation of an organisation from some sort of failure of its information technology systems and supporting processes.

The National Cyber Security Centre's (NCSC) 10 steps to Cyber Security aims to help organisations manage their cyber security risks by breaking down the task of protecting the organisation into 10 components. Adopting security measures covered by the 10 Steps reduces the likelihood of cyber-attacks occurring and minimises the impact to your organisation when incidents do occur. Understanding what you are trying to protect against is essential to managing cyber security risk.

In the past 18 months, we have seen the cyber-crime threat landscape amplified by the impact of the Covid-19 pandemic as cyber criminals seek to capitalise on the disorder. Our recent 2021 survey highlighted that 20 per cent of organisations had experienced a cyber-attack over this period (https://www.rsmuk.com/real-economy/cybersecurity).

The audit was carried out primarily through meetings with key staff members, along with review of documentation relevant to the scope of the review.

Conclusion

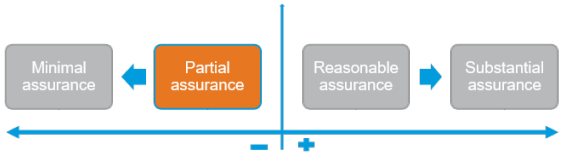
Overall, we identified a number of controls designed to protect the information systems network. Whilst key controls exist, a range of important control improvements are necessary.

This review identified 14 areas where controls require enhancement, resulting in seven 'medium', and seven 'low' priority management actions.

Internal audit opinion:

Taking account of the issues identified, the Service can take partial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Action is needed to strengthen the control framework to manage the identified risk(s).



Key findings

We identified the following weaknesses in the control framework resulting in one high and six medium priority actions:

Management has informed us that there is no regular scheduled scanning in place to scan all files downloaded on the network. This increases the risk of Staffordshire Fire suffering from a successful cyber-attack. **(Medium)**

The Service has a number of key policies and procedural documents which are either outdated, require review, or require additional content. These include: the IT Acceptable Use Policy, the Business Continuity Plan, the IT Incident Management procedural document, and the Information Backup and Restore Policy. There is also no documentation outlining the agreed procedures for backup testing and recovery.

The absence of up-to-date policies and procedures increase the risk that staff fail to follow the correct working practices, leading to cyber controls being bypassed and risks such as cyber-attacks materialising. **(2 x Medium)**

There are no Intrusion Detection or Prevention tools in place, or Active Directory (AD) monitoring of information such as brute force login attempts, login attempts from unusual locations or login attempts that fail 2-factor authentication. Without these monitoring tools there is a risk that repeated attempts of unauthorised access to the network goes unnoticed resulting in a successful cyber-attack. **(Medium)**

The Service does not have defined Recovery Point Objectives (RPOs) or Recovery Time Objectives (RTOs). The absence of agreed RPOs and RTOs increases the likelihood of the recovery of systems and data not meeting the requirements of the Service, leading to prolonged periods of disruption for critical services. **(Medium)**

The Service has not defined its minimum cyber security standards requirements for third-party suppliers. The lack of clarity regarding the minimum standards increases the risk that the Service engages with a third party without the appropriate level of cyber security safeguards in place. This could lead to cyber security breaches, significant operational and reputational harm. **(Medium)**

Whilst vulnerability scans are performed, they do not scan the external network for vulnerabilities, and only scan endpoints. In addition, no evidence was provided to show that all identified vulnerabilities were resolved within acceptable timeframes.

Additionally, annual network penetration tests are not undertaken. There is a risk that there are known vulnerabilities on the Service's network which have not been promptly remediated, leading to those vulnerabilities being exploited in a cyber-attack. **(Medium).**

A full breakdown of all weaknesses and findings identified has been included in Section 2 of the report below.

Examples of good practice identified during the audit include the following:

The Service has in in place a Protective Security Steering Group (PSSG) which helps to identify potential security threats, with regular agenda items to discuss current threats and service standards.

There is a mandatory annual formalised training course called Protecting Information essentials, delivered through the online learning platform LearnPro. At the time of review compliance was 85.2%.

There is an Active Directory password policy in place which allows for single-sign, multi-factor authentication, password deny lists and specific password requirements.

The Service uses ManageEngine to manage the patches across all of its software. This automatically scans the network for software and their updates. This patches third party applications, as well as servers and endpoint patches. In addition, a register is maintained which shows the software licenses for each piece of software and when each requires renewal.

There is a documented ICT Change Management Policy in place which contains the process for requesting and implementing changes, as well as the process for implementing emergency changes.

There is an established standard build for all Staffordshire devices, which is strictly controlled. Deviations from the standard build must be requested through an IT support ticket, and the application must be approved. The ability to install unauthorised software is blocked.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Area: Malware scanning				
Control	*Missing Control* Files are regularly scanned for malware.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	Whilst we can confirm that real time scanning is utilised to scan all downloaded and altered files, management has informed us that there is no regular scheduled scanning in place to scan all files downloaded on the network. If network files are not subject to regular malware scans, then there is a risk that if dormant malware contain exist, or if malware was missed by the real time scanner, these files may not be detected for an extended period of time, increasing the probability of a data breach and successful cyber-attack. Ultimately, this could cause major operational, financial, or reputational harm.			
Management Action 1	We will ensure that all files are regularly scanned as part of a full scheduled scan.	**Responsible Owner:** Richard Evanson	**Date:** March 2023 This was completed and demonstrated during the audit.	**Priority:** Medium

Area: Policies and Procedures				
Control	*Missing Control* The Service has a suite of up-to-date policies and procedures covering all areas relating to cyber risk.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We reviewed the following policies and procedures to ensure they were up-to-date and included relevant information: • IT Acceptable Use Policy; • ICT Business Continuity Plan; • IT Disaster Recovery Plan; and • Information Backup and Restore Policy. From our review, we noted that the IT Acceptable Use Policy and the Information Backup and Restore Policy had not been reviewed since August 2016, and the ICT Business Continuity Plan (BCP) since January 2019. Without an up-to-date set of policies and procedures, there is an increased risk that staff fail to follow the correct procedures, leading to critical processes (such as the ICT BCP) not working as intended. This could lead to prolonged periods of operational disruption for critical services and may cause significant harm and reputational damage to the Service. Inspection of the Information Backup and Restore Policy confirmed that it does not contain key information such as what backups were required, backup schedules and frequency; where backups should be stored; recovery point retention periods; and the requirement to re-run failed backups. There is a risk that IT staff may not be aware of the appropriate backup procedures to follow, leading to backup failures which would impair the Service's ability to recover systems and data from backups. We also found that the document states that regular backup test restores should be completed, but we confirmed through discussion with management that the Service is not currently undertaking any regular restore testing of backups. The lack of any backup restoration testing increases the risk that Staffordshire may not be able to effectively recover all necessary systems and data using their backups, if required to do so. This could lead to a prolonged period of disruption to critical services, leading to harm and reputational damage to the Service. We also reviewed the IT Disaster Recovery (IT DR) procedural document, but noted the document was still in development and did not include details about Incident Management procedures in the event the IT DR process is invoked. Without documented IT DR plan with supporting Incident Management procedures in place, there is a risk that the staff may not follow the correct procedures in responding to a serious IT incident, which could lead to a prolonged period of service downtime, potential causing harm and reputational damage to the Service.			
Management Action 2	2a) We will review and update the IT Acceptable Use Policy, the ICT Business Continuity Plan, and the Information Backup and Restore Policy.	**Responsible Owner:** Richard Evanson	**Date:** October 2023	**Priority:** Low

Area: Policies and Procedures				
	2b) We will review, update, and approve these policies on an annual basis.			
Management Action 3	We will update the Information Backup and Restore Policy to include the following: • Backup selections; • Backup schedule; • Backup frequency; • Where backups are stored; • Recovery point retention periods; • Re-running failed backups; and • Requirement to perform regularly scheduled test restorations from backups.	**Responsible Owner:** Tim Maslin Richard Evanson	**Date:** October 2023	**Priority:** Medium
Management Action 4	We will update, review, formally approve and communicate the ICT Disaster Recovery document. The Incident Management section will be updated to include the following: • Definition of an incident and how to identify an incident; • How to report upon incidents; • Prioritisation of incidents; • Roles and responsibilities of key persons involved Disaster Recovery procedures; and • Communication plan including relevant contact details.	**Responsible Owner:** Richard Evanson	**Date:** October 2023	**Priority:** Medium

Area: Active Directory Monitoring				
Control	*Missing Control* The Service currently utilises Intrusion Detection and Prevention (IDS and IPS) tools, including monitoring of Active Directory (AD).		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	We inquired with Management to ascertain whether any IDS and IPS tools are used to monitor or block suspicious activity and connections, including the monitoring of Active Directory (AD) for activity such as: • Multiple Login attempts, or those that fail 2-factor authentication; • Brute forcing of account passwords; and • Login attempts from unusual geographical areas. We were informed by Management that no such tools are in place and there is currently no baseline level of activity to establish what the Service would expect 'normal' levels of activity to look like. This increases the risk that abnormal user activity would be difficult to identify, leading to cyber-attacks not being identified promptly and remediated In addition, without the use of IDS and IPS tools, there is a risk that Management will not be alerted to a potential cyber-attack attempt, resulting in the lack of an appropriately swift response to mitigate such an attack. This could result in the Service being the victim of a successful cyber-attack, with the associated service disruption and reputational damage this may cause.			
Management Action 5	We will implement monitoring of suspicious connections onto the network from a set baseline of 'normal', including monitoring of AD. This monitoring could include activity such as: • Multiple Login attempts, or those that fail 2-factor authentication; • Brute forcing of account passwords; • Login attempts from unusual geographical areas. The use of IDS and IPS tools should be considered to actively prevent potential attacks from progressing.	**Responsible Owner:** Richard Evanson	**Date:** June 2024	**Priority:** Medium

Area: Recovery Point Objectives (RPOs)				
Control	*Missing Control* The Service has clearly defined and documented Recovery Point Objectives (RPOs).		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	We reviewed documentation provided to determine whether the Service had defined its RTOs and RPOs. The RTO is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs, and the RPO is the maximum acceptable amount of data loss the business can tolerate following a failure or disaster. We found that the Service has a document titled '*Impact Levels Corp BIA'*, most recently updated in March 2022, which sets out the RTOs for each of the key functions within the Service. However, we were unable to confirm that the Service had defined its RPOs as this is not documented. Without defining the RPOs for the key functions the service may be unaware of what a tolerable level of data loss is in the event of a disaster and may not be able to recover data in line with operational requirements, leading to data loss, operational disruption and reputational damage.			
Management Action 6	We will update the Business Continuity documentation to include the identification of Recovery Point Objectives (RPOs). In addition, the IT Disaster Recovery plan should include the agreed RPO to ensure that services would be recovered in line with the agreed objectives.	**Responsible Owner:** Richard Evanson	**Date:** October 2023	**Priority:** Medium

Area: Third-Party Minimum-Security Requirements				
Control	*Missing Control* The Service has a documented policy defining the minimum-security standards which are required of third-party suppliers to the Service.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We found through inspection of the third-party contract register that suppliers are selected using procurement frameworks such as the Crown Commercial Service Framework and HealthTrust Europe ICT Solutions Framework. Therefore all suppliers meet security and monitoring standards as set out by the framework at the point of initial procurement. However, we were unable to confirm that the Service has documented the monitoring procedures it undertakes to ensure that minimum standards are being maintained by third-party suppliers. Without defining the process and those responsible for undertaking it, there is a risk that third parties in the supply chain may not be maintaining adequate cyber security controls, which may leave the Service exposed to an increased threat of cyber-attack.			
Management Action 7	We will document the procedures in place for monitoring and ensuring third-party suppliers are meeting and maintaining the minimum cyber-security standards.	**Responsible Owner:** Richard Evanson Fiona Peel	**Date:** August 2023	**Priority:** Medium

Area: Vulnerability scanning and penetration testing.				
Control	*Missing Control* Vulnerability scans, and penetration tests take place across the entire network.	**Assessment:** **Design** **Compliance**	 × N/A	
Findings / Implications	From inspection of the ICT Patching and Vulnerability Management Policy, we confirmed that it does not include any details regarding the approach to vulnerability scanning. Additionally, management has informed us that there are no regular penetration tests which are scheduled to occur or have occurred recently. However, further inquiry conformed that the Service uses Nessus as a tool for performing vulnerability scans. From inspection of the Nessus vulnerability scanning reports, and from inquiry of management, we confirmed that whilst vulnerability scans are being performed, these only scan the network endpoints and do not scan the external network for vulnerabilities. Consequently, the scans would not include some of the critical network infrastructure equipment, such as the firewall. In addition, we confirmed that although the internal vulnerabilities are being identified, there was no clear mechanism for ensuring that they are addressed in a timely manner and we were unable to obtain evidence of the resolution of the identified vulnerabilities, including the setting of agreed SLA recovery times for addressing the various severity of vulnerabilities. There is a risk that there are known vulnerabilities on the Service's network which management are unaware of and that these vulnerabilities could be exploited via a cyber-attack, leading to significant operational, financial and reputational harm.			
Management Action 8	We will update the ICT Patching and Vulnerability Management Policy to include the requirement to schedule and perform an annual penetration test with a chosen vendor. In addition, the Policy should also outline the approach to vulnerability scanning across the entire network, including requirements to scan internal and external devices, the frequency of these activities and the mechanisms for ensuring that vulnerabilities are assigned a resolution target date depending on the criticality of the vulnerability and tracked through to completion.	**Responsible Owner:** Richard Evanson	**Date:** October 2023	**Priority:** Medium

Area: Phishing and Whaling Exercises				
Control	*Missing Control* The Service has a documented plan in place setting out the phishing and whaling exercises it plans to undertake over the next financial year.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	Through discussion with Management, we determined that whilst the Service offers some cyber related training for staff, they are not currently undertaking any phishing or whaling exercises to help establish the overall effectiveness of that training. Management informed us that there is no budget to undertake any exercises within the remainder of this financial year (year ending 31 March 2023), however phishing and whaling exercises have been factored into the budget for the next financial year. We found that whilst the Service intends to undertake these exercises, it currently has no documented plan in place detailing key information such as resourcing requirements and timescales. Without this, the Service may risk not allocating the correct resource requirement and risk slippage in the delivery of these exercises. This could lead to an ineffective programme of cyber related training at the Service, leading to staff being unaware of cyber related threats and increasing the likelihood of a successful cyber-attack.			
Management Action 9	We will design a plan for phishing exercises to take place next year, outlining the resources required to implement this, the dates of these exercises and an action plan for addressing the issues identified following these exercises,	**Responsible Owner:** Richard Evanson	**Date:** October 2023	**Priority:** Low

Area: Third Party Contracts – Sample Testing				
Control	*Missing Control* The Service has signed contracts in place for all third-party suppliers.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We selected a sample of five contracts from the Service's contract register ('Tally Sheet'). We requested a copy of the contracts to ascertain whether they contained suitable recourse for failure to meet the Service Level Agreements (SLAs), as well as ensuring that contracts have been signed by both parties and retained. We were only provided with four out of the five contracts selected, as the remaining contract could not be located at the time of review. Of the four contracts we confirmed that each of them had agreed upon recourse for a failure to meet SLAs, and where applicable metrics that would be monitored and reported upon. We also reviewed each of the contracts provided to determine if they were all signed by both parties. We found only two of the contracts contained signatures from both parties. Without retaining a signed copy of each contract, the Service may find itself unable to legally challenge the third-party on the delivery of their SLAs, which could lead to service failures, cyber breaches and reputational damage to the Service.			
Management Action 10	We will ensure that a signed copy of each contract is retained.	**Responsible Owner:** Fiona Peel Richard Evanson	**Date:** July 2023	**Priority:** Low

Area: Hardware Asset Management				
Control	*Missing Control* There is regular review of hardware asset registers to ensure they remain accurate.		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	The Service maintains a hardware asset register using a tool called SPPEMS, where hardware asset data is manually inputted and maintained. Management has informed us that there is no regular review of the hardware assets owned by Staffordshire. Without a regular review of hardware assets, there is a risk that the hardware asset register is inaccurate and fails to reflect the current IT estate. This could lead to some assets no longer being where they are expected to be, making it difficult to detect loss or theft of devices. In addition, the Service cannot adequately protect their IT assets if they fail to have full visibility of the assets they manage. This could lead to some devices not being maintained in line with agreed cyber security controls, leading to an increased likelihood of cyber-attack.			
Management Action 11	We will ensure that hardware asset registers are regularly reviewed and updated. This could be achieved through automation of hardware monitoring, utilising tools which scan the network for devices, or regular manual reviews of hardware assets using the current tool.	**Responsible Owner:** Richard Evanson	**Date:** December 2023	**Priority:** Low

Area: Auditing of administrator accounts				
Control	*Missing Control* Administrator accounts, including Domain and Firewall admins have appropriate change monitoring, and auditability.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	From inspection of the firewall administrator accounts, we noted that there is a general 'Admin' account which can be accessed and used by multiple administrators. In addition, Management has informed us that there is no audit trail of Domain Admin account activity. There is a risk that unauthorised changes could be made to the firewall using the shared account and the lack of accountability could make it difficult to determine which administrator has made the changes. This could lead to uncontrolled changes being made to the firewall which could potentially leave the network vulnerable to cyber-attack. Additionally, if there is no audit trail of changes made by Domain Admins accounts then there is a similar risk that unauthorised activity from privileged accounts could go undetected, which increases the risk of cyber-attack.			
Management Action 12	We will ensure that there are no shared Administrator accounts on the firewall, and all accounts are identifiable to a single user. Furthermore, we will implement an audit trail of for Domain Admins, which alerts management for any changes or unusual activity.	**Responsible Owner:** Richard Evanson	**Date:** December 2023	**Priority:** Low

Area: Patch testing				
Control	*Missing Control* All patches are tested prior to release.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	The ICT Patching and Vulnerability Management Policy states that "*all patches must first be tested on a sample group of machines or, in the case of firmware updates, a non-critical piece of equipment*". Management confirmed that this is not taking place. From inquiry of Management we confirmed that due to the size of the organisation, this would add a layer of complexity, and may not be feasible with the resources available. However, it was not clear where this decision had been made and whether it had been agreed by the Service. There is a risk that if patches are not tested prior to release, then faulty patches may be deployed, which could cause operational disruption to the Service and may also introduce vulnerabilities on the network which could be exploited by a cyber-attack.			
Management Action 13	We will ensure that patches are tested prior to release in line with the ICT Patching and Vulnerability Management Policy. Alternatively, if this is not completed due to resourcing constraints, this risk should be added to the IT risk register and tracked. The ICT Patching and Vulnerability Management Policy will be updated to reflect the agreed procedures.	**Responsible Owner:** Richard Evanson	**Date:** October 2023	**Priority:** Low

Area: Log Retention Policies				
	Missing Control There is a Log Retention Policy in Place.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	Management has informed us that there is no Log Retention Policy in place at Staffordshire, which details how long various data types should be held for on company systems. Security-related event logs seek to provide comprehensive information for detecting and reacting to security incidents. Typically the logs could be used to track the following activities: • User account and application/software involved in the activity; • Time of the activity; and • The outcome of the activity (success, failure, error). There is a risk that if there is no Log Retention Policy in place that Management will not be aware of how long to keep various types of stored data. This could result in excessive amounts of data being stored which could lead to increased storage costs or that data is being stored beyond the needs of Service, which could lead to breaches of the GDPR if personal data is involved. This in turn could lead to fines and reputational damage.			
Management Action 14	Management will implement a Log Retention Policy which includes details regarding how long each type of stored data should be held for on Staffordshire's systems.	**Responsible Owner:** R Evanson	**Date:** December 2023	**Priority:** Low

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

NCSC 10 Areas	Agreed actions		
	Low	Medium	High
Risk Management	0	0	0
Engagement and Training	1	0	0
Asset Management	1	0	0
Architecture and Configuration	0	0	0
Vulnerability Management	1	1	0
Identity and Access Management	1	1	0
Data Security	0	1	0
Logging and Monitoring	1	0	0
Incident Management	0	2	0

Supply Chain Security	1	1	0
General	1	1	0
Total	**7**	**7**	**0**

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risk:

Objective of the risk under review	Risks relevant to the scope of the review
To provide assurance that the processes in place to manage cyber security risk are effective.	Loss of information, risks from inappropriate and malicious access, viruses and malware and of legal action/ loss of reputation due to inappropriate storage of/ sharing of personal data.

When planning the audit, the following areas for consideration and limitations were agreed:

The National Cyber Security Centre's (NCSC) 10 steps to Cyber Security aims to help organisations manage their cyber security risks by breaking down the task of protecting the organisation into 10 components. Adopting security measures covered by the 10 Steps reduces the likelihood of cyber-attacks occurring and minimises the impact to your organisation when incidents do occur. Understanding what you are trying to protect against is essential to managing cyber security risk. The review will focus on the following scope areas and associated controls at a high level:

1. **Risk Management**
   - The risk management process (identification, assessment, treatment, monitoring).
   - Senior management leadership for IT Risk Management, including Management Information ('MI') and Key Risk Indicators ('KRIs') used to inform decision makers on the performance of key IT controls.

2. **Engagement and training**
   - User education and awareness in respect of IT Security.
   - Phishing and whaling prevention.

3. **Asset management**
   - Maintenance of software and hardware inventories.
   - Maintenance of an Information Asset Register (IAR).

4. **Architecture and configuration**
    - Perimeter protection, including application of firewalls, firewall rules settings and change management.
    - Application of Intrusion detection and prevention.
    - Standard baseline builds of managed devices.

5. **Vulnerability management**
    - Software update strategy for managed devices.
    - Vulnerability management procedures, including prioritization of critical vulnerability remediation.

6. **Identity and access management**
    - Definition or policy of identity and access management.
    - Authorisation model and procedures (e.g. account creation, deletion and amendment) for users.
    - Authentication for end user accounts, including password policy.
    - Restrictions to privileged accounts (e.g. administrative accounts).
    - Monitoring of account usage and accesses.
    - Rules around known third-party access to the internal network.

7. **Data security**
    - Restrictions on use of removable media.
    - Use and upkeep of anti-malware software.
    - Use of file scanning.
    - Backup policies and procedures.
    - Data disposal process (hardware).

8. **Logging and monitoring**
    - The monitoring, alerting and reporting processes.
    - Log retention policy and procedures.
    - Access controls to logs.
    - Monitoring of Active Directory Activity.

9. **Incident management**
    - Incident management and reporting process, as well as lessons learnt.
    - Detection of security breaches or unauthorised access attempts.
    - IT Disaster Recovery procedures.

10. **Supply Chain Security**
    - Identification of third-party providers and the services they provide.
    - Processes and procedures in place to assess the security capabilities and management of cyber risk by third party providers.

- Third-party access to infrastructure and information.

Limitations to the scope of the audit assignment:

- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of IT/cyber security.
- The approach taken for this review will be to validate the design of key controls and will not include all monitoring controls.
- We will be testing only selected key controls and on a sample basis only.
- We will not perform penetration tests and vulnerability assessments however we will review the results of tests undertaken by independent service providers.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the IT environment, and it will be necessary for management to consider the results and make their own judgement on the risks and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

Debrief held	25 January 2023
Draft report issued	14 February 2023
Revised Draft report issued	22 March 2023
Responses received	3 May 2023
Final report issued	3 May 2023

Internal audit Contacts	Daniel Harris, Head of Internal Audit Angela Ward, Senior Manager Kishan Patel, Assistant Manager
Client sponsor	Richard Evanson, Head of ICT
Distribution	Richard Evanson, Head of ICT

FOR FURTHER INFORMATION CONTACT

Paul O'Leary

Technology Risk Assurance Partner

T: +44 (0) 7498 929 396

E: Paul.O'Leary@rsmuk.com

RSM Risk Assurance Services LLP
Fifth Floor, Central Square, 29 Wellington Street,
Leeds, LS1 4DL

Richard Curtis

Technology Risk Assurance Senior Manager

T: +44 (0) 7818 002 534

E: Richard.Curtis@rsmuk.com

RSM Risk Assurance Services LLP
25 Farringdon Street, London, EC4A 4AB

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Staffordshire Fire and Rescue and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.