ROYAL BERKSHIRE FIRE & RESCUE SERVICE

Internal Audit Progress Report

29 July 2026

CONTENTS

Appendices

KEY MESSAGES

The internal audit plan for 2025/26 was approved by the Audit and Governance Committee at the March 2025 meeting. This report provides an update on progress against the plan and summarises the results of our work to date.

2025/26 Internal Audit Plan:

We have issued the four remaining final reports as part of the internal audit plan from the 2025/26 internal audit plan since the last Audit and Governance Committee meeting in March 2026:

- Procurement **(Reasonable Assurance)**
- Follow Up **(Little Progress)**
- IT Security **(Reasonable Assurance)**
- Business Continuity **(Reasonable Assurance)**

A summary of the outcome of these reviews is provided in Section 1. This completes the 2025/26 plan. **[To discuss and note]**

2026/27 Internal Audit Plan

The draft Internal Audit Plan for 2026/27 is included on today's agenda with audits due to commence in September 2026. **[To discuss and approve]**

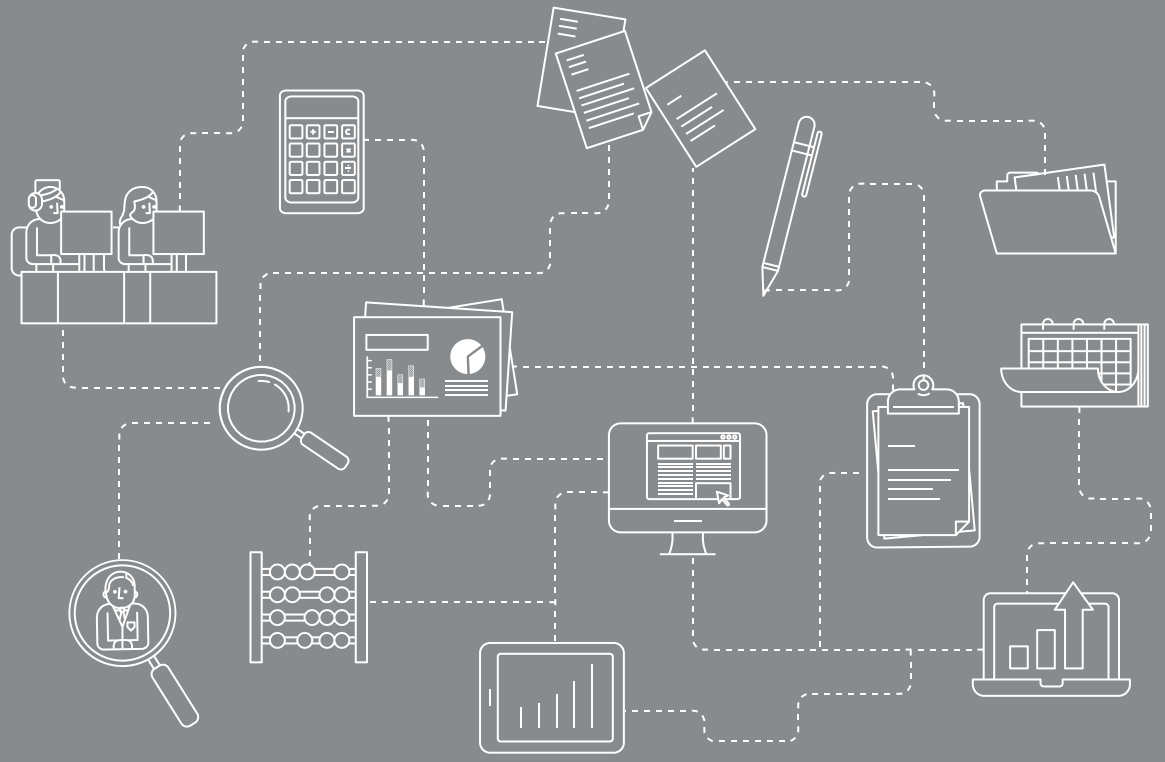
Details of the progress made against the internal audit plans are included at Appendices A and B. **[To note]**

2025/26 Annual Report

The 2025/26 Annual Report, including our year end opinion, is also included on today's agenda. **[To discuss and note]**

Final Reports

01



1 FINAL REPORTS

1.1 Summary of final reports being presented to this Committee

This section summarises the 2025/26 reports that have been finalised since the last meeting.

Assignment	Opinion issued	Actions agreed			
		A	L	M	H
Procurement (7.25/26) Overall, we found that the Service has well designed procurement controls, with clear policies aligned to the Procurement Act 2023, consistent use of tender processes, and good evidence of value for money across sampled contracts. Transparency requirements were met, purchase order compliance was strong, and quarterly reporting to the SPB supported effective oversight of procurement activity. However, we identified some weaknesses in the control framework. Specifically, the contract register was not fully up to date, with expired and extended contracts not accurately reflected, increasing the risk of decisions being based on incomplete information. Whilst we noted that there was a comprehensive provision of training from the Procurement team, the results from our staff survey included that awareness of responsibilities under the Procurement Act 2023 was inconsistent, with some respondents unaware of the new framework, the training available, or the requirement to notify Procurement of contract terminations. Awareness of existing training materials appeared low, pending the full rollout of the Learning Management System. **Root cause:** Procurement responsibilities and record-keeping requirements have not been consistently embedded across the Service.	Reasonable Assurance	-	-	2	-
Follow Up (8.25/26) Of the six management actions followed up, three had been implemented and the remaining three had been partially implemented. In our opinion, the Service has demonstrated little progress in implementing agreed management actions. Based on our findings, we have agreed one high and two medium priority management actions. **Root cause:** Management actions were not subject to sufficiently robust implementation oversight.	Little Progress	-	-	2	1
IT Security (9.25/26) The review identified that the Service has a number of established technical and operational controls in place to manage IT and information security risks. These include the use of centralised security tooling,	Reasonable Assurance	-	5	4	-

monitoring of key systems, regular risk escalation through senior leadership governance, and the operation of backup, disposal, and training activities in practice.

The issues identified through this review primarily relate to the formalisation and documentation of existing practices, rather than the absence of controls. In several areas, processes are operating but are not consistently supported by documented procedures, defined governance expectations, or clear evidence of oversight. This affects the Service's ability to demonstrate consistency, accountability, and repeatability of control operation.

The majority of the agreed actions relate to the need to document or formalise policies, procedures, or governance arrangements, including areas such as asset and information management, data disposal, backup management, logging and monitoring, phishing simulations, and follow up processes.

Root cause: Existing security controls have not been fully formalised through documented governance and procedures.

Business Continuity (10.25/26)

We identified several controls that were well-designed and operating effectively, considering the emerging maturity of the business continuity function. The Service has clear and comprehensive Business Continuity Policy and Guidance documents that set out roles, responsibilities, and governance expectations, and these are readily accessible to staff. Strong oversight is also in place through the Business Continuity Steering Group, Operational Learning and Assurance Board and related governance structures, which provide appropriate challenge, escalation routes, and support for embedding the Business Continuity Management System. The exercising programme is well structured, with quarterly themed scenarios communicated through Siren SharePoint, and we confirmed that guidance for coordinated response is clearly articulated across several key documents. In addition, critical suppliers were broadly consistent with what we would expect for the sector, with continuity considerations evident in all applicable contracts reviewed.

Reasonable Assurance	-	5	2	-

However, we did identify some weaknesses in the current control framework. These include inconsistent completion of Business Impact Assessments and Business Continuity Plans (BCPs) and gaps in exercising compliance. We also noted instances where learning from exercises was not reflected in updates to BCPs, and an organisation wide assessment of critical functions had not yet been completed. These gaps limit the Service's ability to fully assure its resilience arrangements and highlight the need for continued strengthening of the Business Continuity Management System.

Root cause: Business continuity requirements have not been consistently embedded across the Service.

Appendices

02

APPENDIX A: PROGRESS AGAINST THE INTERNAL AUDIT PLAN 2025/26

Assignment	Status / Start Date / Opinion issued	Actions agreed				Target Committee meeting per IA plan (or revised Committee)	Actual Committee meeting
		A	L	M	H		
Service (Non-Corporate Risks) Risk Management and Governance of Service Plans	Final – Reasonable Assurance (RM) / Partial Assurance (Gov)	-	5	5	-	October 2025 (July 2026)*	January 2026
Payroll Provider – Dataplan (now IRIS)	Final – Reasonable Assurance	-	4	3	-	January 2026 (March 2026)*	January 2026
Equality Impact Assessments	Final – Reasonable Assurance	-	3	4	-	March 2026	January 2026
Firefighter Pensions Administration (WYPF)	Final – Partial Assurance	-	8	3	2	March 2026	March 2026
Key Financial Controls	Final – Substantial Assurance	-	-	-	-	March 2026	March 2026
Health and Safety – Contaminants	Final – Reasonable Assurance	-	2	3	-	March 2026	March 2026
Procurement	**Final – Reasonable Assurance**	**-**	**-**	**2**	**-**	**March 2026 (July 2026)***	**July 2026**
Follow Up	**Final – Little Progress**	**-**	**-**	**2**	**1**	**July 2026**	**July 2026**
IT Security	**Final – Reasonable Assurance**	**-**	**5**	**4**	**-**	**July 2026**	**July 2026**
Business Continuity	**Final – Reasonable Assurance**	**-**	**5**	**2**	**-**	**July 2026**	**July 2026**

* The timing of these audits have been changed to accommodate staff availabilities (we have not noted any issues with these timing changes).

APPENDIX B: PROGRESS AGAINST THE INTERNAL AUDIT PLAN 2026/27

Assignment	Status / Opinion issued	Actions agreed				Target Committee meeting (as per IA plan / change controls)	Actual Committee meeting
		A	L	M	H		
Information Governance (Retention Schedules)	Scheduled – September 2026					January 2027	-
Payroll Provider - Zellis	Scheduled – November 2026					January 2027	-
H&S Management of Contractors	Scheduled – November 2026					January 2027	-
Firefighter Pensions Administration (WYPF)	Scheduled – Novemeber 2026					January 2027	-
Key Financial Controls	Scheduled – January 2027					April 2027	-
Risk Management and Governance	Scheduled – February 2027					April 2027	-
Worker Protection Act – Action Plan	Scheduled – February 2027					April 2027	-
Follow Up	Scheduled – February 2027					April 2027	-
Cyber	TBC – Q4					July 2027	-

* The timing of these audits have been changed to accommodate staff availabilities (we have not noted any issues with these timing changes).

APPENDIX C: OTHER MATTERS

Changes to the plan

Any requested changes to the timing of audits, or to the audits themselves will be reported to future committee meetings.

Added value work

We have issued the following client briefings since the last Audit Committee:

- Emergency Services News Briefing – June 2026
- RSM Emerging Risk Radar – Spring 2026
- Quality Assurance and Improvement Programme
- RSM UK External Quality Assessment

External Quality Assessment

RSM operates in accordance with the Global Internal Audit Standards (GIAS), which require internal audit to undertake an External Quality Assessment (EQA) at least once every five years. Our last assessment in 2021 achieved the highest rating of “generally conforms”. Our next EQA is scheduled to commence in October 2026.

Since our last EQA, the Institute of Internal Auditors (IIA) has issued new standards, effective from January 2025. The new GIAS 8.4 states that: “The chief audit executive must develop a plan for an external quality assessment and discuss the plan with the board. The external assessment must be performed at least once every five years by a qualified, independent assessor or assessment team.”

Our EQA approach aligns with the Chartered IIA guidance for multi-client providers.

- We will commission an external assessor to perform a review of the design of our internal audit methodology, and arrangements to meet the GIAS. The review will cover all 15 Principles and 52 Standards across the Domains of the GIAS, from a design perspective.
- Our EQA will review the design of our arrangements to meet the requirements of the Application Note, Global Internal Audit Standards in the UK Public Sector.
- Following the assessment, RSM will receive detailed feedback and will share a high-level conformance statement of the results with clients.

We will appoint an external independent, qualified assessor through a competitive tender process during the summer. To discuss EQAs further or our approach in more detail, please contact your Head of Internal Audit.

Further detail on our approach is available in our client briefing External Quality Assessment.

FOR FURTHER INFORMATION CONTACT

Dan Harris, Partner and Head of Internal Audit

Email: Daniel.Harris@rsmuk.com

Telephone: 07792 948767

Zoe Walker, Managing Consultant

Email: Zoe.Walker@rsmuk.com

Telephone: 01245 454106

AUDIT OUTCOME OVERVIEW - PROCUREMENT

Background: We undertook a review of Procurement as part of the approved 2025/26 internal audit plan. The objective of the review was to assess the adequacy and effectiveness of controls surrounding procurement purchases of goods and services through contracts awarded via tender and to determine how the organisation ensures that value for money is considered.

Procurement responsibilities are led by the Senior Procurement Specialist, with operational input from Contract Managers across the organisation. Governance for procurement activity is overseen by the Fire Authority, with day to day responsibilities delegated to the Deputy Head of Finance and Procurement and the Procurement Team.

Procurement processes are documented within the Contract Standing Orders (2025) which set out procurement objectives, approval thresholds, delegated authority limits and waiver procedures. The framework incorporates the transparency, competition and value for money principles mandated under the Procurement Act 2023. Although tendering activity has started under the new framework, full end to end procurement under the Procurement Act 2023 had not yet taken place at the time of audit. Draft contracts were in place for certain procurements, such as the Hard FM tender, but these had not yet been completed or formally awarded. As a result, the organisation has limited practical experience of applying the full lifecycle of the new regime in practice.

Meetings are held between the Procurement Team and operational leads to monitor contract activity, and quarterly reporting is provided to the Strategic Performance Board (SPB) to highlight contract awards, compliance and supplier spend. The service also publishes payments over £500 and procurement card transactions in line with statutory transparency requirements.

As of December 2025, the organisation managed 146 active contracts. Ten tender waivers were raised between June 2024 and January 2026, totalling £331k. For the year to date, £15.9m had been spent across 3,491 purchase orders, all supported by a valid purchase order.

Conclusion: Overall, we found that the Service has well-designed procurement controls, with clear policies aligned to the Procurement Act 2023, consistent use of tender processes, and good evidence of value for money across sampled contracts. Transparency requirements were met, purchase order compliance was strong, and quarterly reporting to the SPB supported effective oversight of procurement activity.

However, we identified some weaknesses in the control framework. Specifically, the contract register was not fully up to date, with expired and extended contracts not accurately reflected, increasing the risk of decisions being based on incomplete information. Whilst we noted that there was a comprehensive provision of training from the Procurement team, the results from our staff survey included that awareness of responsibilities under the Procurement Act 2023 was inconsistent, with some respondents unaware of the new framework, the training available, or the requirement to notify Procurement of contract terminations. Awareness of existing training materials appeared low, pending the full rollout of the Learning Management System.

Internal audit opinion:

Audit themes:

We identified the following exceptions, resulting in the agreement of two medium priority management actions:

Contracts Nearing Expiry: Through review of a sample of five contracts that appeared outdated in the Contracts Register, we found that two expired contracts and three updated contracts had not been correctly reflected in the contract register at the time of review, despite end dates having passed or new agreements being in place. The Senior Procurement Specialist advised that monthly reviews are undertaken, but recent updates had not yet been completed due to ongoing procurement activity. **(Medium)**

Awareness of Procurement Requirements: Whilst we appreciate that the Procurement team have provided training to relevant individuals within the Service, a procurement questionnaire was completed as part of the audit and the results contradicted the evidence reviewed with regards to indicated gaps in staff awareness, with some respondents responding that they were unaware of the Procurement Act (2023), related training, and their responsibility to notify the Procurement Team of contract terminations. While comprehensive training materials had been delivered in 2025 and made available via SharePoint and for inclusion in the new LMS, these had notably not been fully accessed or understood by all staff. **(Medium)**

We noted the following controls to be well designed and operating effectively:

Policy: The updated Contract Standing Orders (CSO) published in February 2025 were approved by the Fire Authority and shared with stakeholders via the website, setting out clear procurement objectives, key roles and responsibilities, and procedural expectations. We noted that the CSO aligns with the 2023 Procurement Act, embedding updated thresholds, digital platform requirements, and the principles of transparency, competition, and value for money.

Financial Regulations: The Service maintains Financial Regulations that clearly outline the requirements for compliance with the limits set out in the CSO policy. We confirmed that the Financial Regulations were last reviewed and updated in February 2025, approved through the Fire Authority's formal governance process, and were made available on the website.

Waivers: Through review of the contracts register, we found that five tender waivers had been raised since February 2025, with values ranging from approximately £15k to £50k. We confirmed that all five waivers used the standard form, included a valid rationale, and were independently reviewed and approved in line with delegated authority under CSO.

Procurement transparency: Through review of the RBFRS website, we confirmed that procurement-related financial information, including payments over £500 and procurement card transactions, is published on a monthly basis in line with the organisation's transparency obligations. All required datasets were available, up to date at the time of review, and clearly accessible to the public.

Central Digital Platform: Through walkthrough of Central Digital Platform (Find a Tender) it was confirmed that the Service had registered onto the platform to access procurement opportunities since February 2025.

Contracts Register: We reviewed the contracts register as of December 2025 and noted that 146 contracts were in place. The register included key information for each contract, including contract type, description of goods and services, contract start and end dates, contract value, supplier name, and supplier details such as company registration information.

Procurement Compliance: Through review of 20 contracts, we found that all 20 followed the intended route to market in line with CSO, and award and selection criteria were correctly applied in 19 cases, demonstrating Value for Money through competition, evaluation scoring, and whole-life costing or price-reasonableness checks. Fully signed contracts were in place for 19 contracts, while the remaining £9.8k purchase (tested due to its proximity to the £10k threshold) had an adequate purchase order raised in accordance with requirements ad was therefore not an identified issue.

KPI reporting: We reviewed the contracts register and noted that no contracts over £5 million were in place; therefore, the annual reporting of Key Performance Indicators (KPIs) required under the 2023 Procurement Act was not applicable. However, the Senior Procurement Specialist advised that KPI reporting is being implemented in the future for high-value contracts to ensure effective performance monitoring, and to promote greater transparency and accountability across the procurement process.

Reporting to Strategic Performance Board (SPB): Contracts awarded on a quarterly basis, along with compliance with the tender processes followed and supplier spend, are reported to the SPB each quarter. Through review of the Q1 and Q2 reports for 2025/26, we confirmed that all awarded contracts were appropriately reported and that compliance with the relevant procurement routes was fully documented and the Service remained within its target.

Procurements just below / above thresholds: Through analysis of supplier payments made since April 2025, we noted that payments totalling £12.9m excluding VAT were made to 395 suppliers. A review of five suppliers confirmed that the route to market was applied in line with CSO, appropriate tender processes were followed, award and selection criteria were correctly applied, Value for Money was demonstrated, and fully signed contracts with key terms were in place.

SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

High	Medium	Low
Immediate management attention is necessary.	Timely management attention is necessary.	There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
1	We will keep the contract register up to date by recording contract expiries, extensions and revised end dates in a timely manner. Any draft extensions or pending updates will be clearly noted in the register to provide transparency on work still in progress.	Medium	Shuvham Bhandari, Senior Procurement Specialist	31 March 2026
2	We will reiterate to staff about the training materials available on the Procurement Act (2023) and highlight their accessibility within the new LMS once implemented, with a focus on the responsibility to notify the Procurement Team of contract terminations in order to support compliance and transparency. Training will continue to be refreshed as appropriate (to capture new changes etc) for all stakeholders.	Medium	Shuvham Bhandari, Senior Procurement Specialist	TBC – dependant on LMS implementation

EXECUTIVE SUMMARY – FOLLOW UP

Background

The review assessed the implementation of all medium priority actions marked as complete by management from the following audits:

- Driving License Checks (1.24/25) – one medium and one high priority action
- Discipline and Grievance Handling (5.24/25) – two medium priority actions
- Risk Management and Governance (8.24/25) – two medium priority actions

The management actions followed up during this review consisted of five medium and one high priority actions. The focus of this review was to allow management to take assurance that medium and high priority actions previously agreed during these reviews have been implemented.

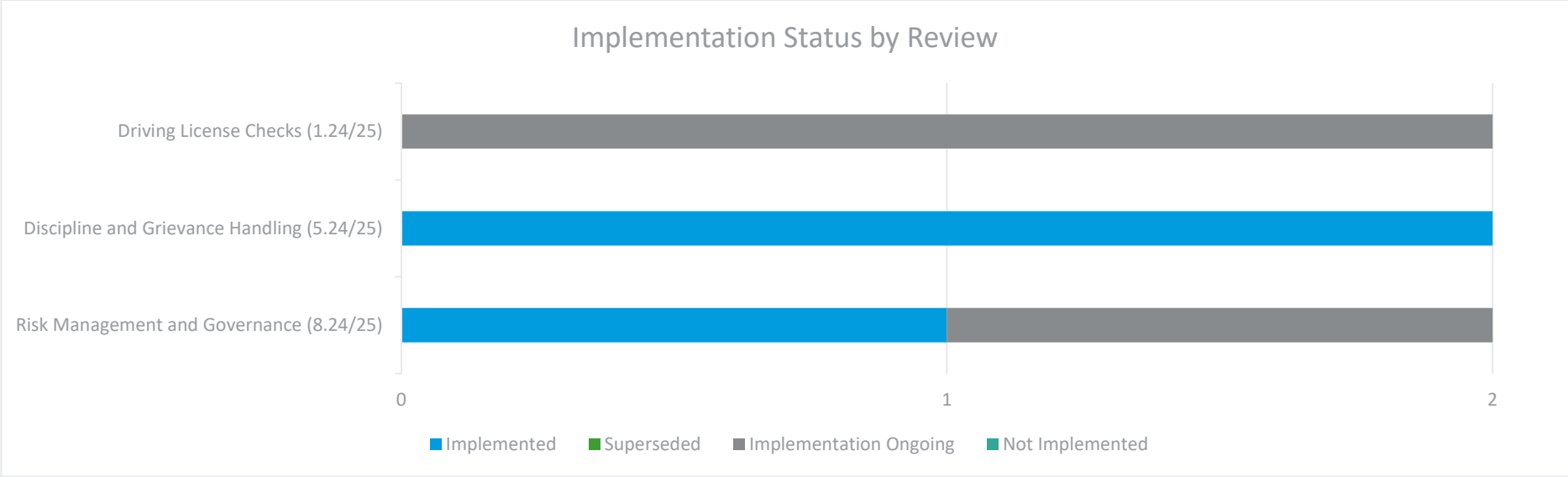
Conclusion

Taking account of the issues identified in the remainder of the report and in line with our definitions set out in Appendix A, in our opinion Royal Berkshire Fire & Rescue Service has demonstrated **little progress** in implementing agreed management actions. We found that three of the actions had been implemented and three had been partly though not yet fully implemented. Based on our findings, we have agreed one high and two medium priority management actions.

Progress on actions

The following table includes details of the status of each management action:

Implementation status by review	Number of actions agreed	Status of management actions				
		Impl. (1)	Impl. ongoing (2)	Not impl. (3)	Superseded (4)	Completed or no longer necessary (1) + (4)
Driving License Checks (1.24/25)	2	0	2	0	0	0
Discipline and Grievance Handling (5.24/25)	2	2	0	0	0	2
Risk Management and Governance (8.24/25)	2	1	1	0	0	1
Total	**6**	**3**	**3**	**0**	**0**	**3**


Implementation Status by Review
Driving License Checks (1.24/25)
Discipline and Grievance Handling (5.24/25)
Risk Management and Governance (8.24/25)
0
1
2
Implemented
Superseded
Implementation Ongoing
Not Implemented

AUDIT OUTCOME OVERVIEW – IT SECURITY

Conclusion:

The review identified that Royal Berkshire Fire and Rescue Service (RBFRS) has a number of established technical and operational controls in place to manage IT and information security risks. These include the use of centralised security tooling, monitoring of key systems, regular risk escalation through senior leadership governance, and the operation of backup, disposal, and training activities in practice.

The issues identified through this review primarily relate to the formalisation and documentation of existing practices, rather than the absence of controls. In several areas, processes are operating but are not consistently supported by documented procedures, defined governance expectations, or clear evidence of oversight. This affects RBFRS's ability to demonstrate consistency, accountability, and repeatability of control operation.

A total of nine management actions have been agreed, comprising four medium priority and five low priority actions. The majority of the agreed actions relate to the need to document or formalise policies, procedures, or governance arrangements, including areas such as asset and information management, data disposal, backup management, logging and monitoring, phishing simulations, and follow-up processes. Taking account of the scope of the review, the nature of the findings, and the absence of high priority issues, management can take reasonable assurance over the arrangements in place to manage IT security risks.

Internal audit opinion:

Minimal Assurance

Partial Assurance

Reasonable Assurance

Substantial Assurance

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

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk(s).

Formalisation of established practices

A recurring theme across the review is that several controls are operating based on established ways of working but are not consistently supported by formally documented procedures. Examples include asset and information management, data disposal, phishing simulation planning, backup management, and logging and monitoring activities. The absence of documentation limits RBFRS's ability to demonstrate consistent application and governance oversight.

Audit themes:

Clarity of ownership and escalation through documentation
In some areas, ownership and escalation routes are understood in practice but are not clearly documented. For example, responsibilities for follow-up training after phishing simulation failures and oversight of disposal evidence are known operationally but not formally defined. This creates reliance on individual knowledge rather than embedded governance.

Improving consistency through governance metadata and review cycles
Several policies and procedures lack complete governance metadata, such as approval details, version control, or defined review cycles. Addressing this will help ensure documentation remains current, aligned to operational practice, and capable of supporting consistent control operation as systems, risks, or personnel change.

Strong technical security baseline
RBFRS has implemented a range of technical controls that provide a solid foundation for managing cyber security risks. This includes centralised endpoint protection, anti-malware tooling, file scanning, and device monitoring. Evidence reviewed confirms that these controls are active and generally operating as intended across the environment.

Effective integration of IT risk into enterprise governance
IT and cyber risks are embedded within the organisation-wide risk management framework and are escalated through established senior leadership governance. Risks above defined thresholds are discussed at Senior Leadership Team meetings, with a focus on risk movement, ownership, and progress of mitigating actions. This supports informed oversight without the need for parallel technology-specific governance forums.

Operational controls working in practice
In several areas, controls were observed to be operating effectively in practice, even where documentation requires strengthening. For example, backup restore testing is performed, hardware is disposed of through approved partners with evidence of secure data destruction, and phishing simulations are conducted with outcomes monitored and follow-up training assigned. These activities demonstrate active risk management rather than reliance on paper controls.

SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

High	Medium	Low
Immediate management attention is necessary.	Timely management attention is necessary.	There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
2	Management will: • Complete the configuration of SDS, including automated reminders, data clean-up and dashboard development; • Assign mandatory Cyber Security and Protecting Information training to all relevant staff within SDS; • Implement routine management reporting of training completion, overdue training and persistent non-completion; and • Compare training completion results against defined compliance expectations.	Medium	Information Governance Manager	31 December 2026
4	Management will define and document a process for assigning, monitoring, and escalating follow-up actions where users fail phishing simulations. The process will treat repeated failures as a performance management matter and set out responsibilities, escalation routes, and completion expectations. The process will include graduated consequences for repeated failures, which may include: • Mandatory refresher training following an initial failure. • Escalation to line management where repeat failures occur. • Increased monitoring or targeted awareness interventions. • Formal performance management or disciplinary action for persistent non-compliance, in line with organisational policies.	Medium	ICT Service Delivery Manager	30 November 2026
5	Management will create and document an Asset and Information Management procedure that defines responsibilities, lifecycle management activities, inventory maintenance expectations, classification requirements, and governance arrangements.	Medium	ICT Service Delivery Manager	31 March 2027

Ref	Action	Priority	Responsible Owner	Date
	The procedure will include the establishment and maintenance of a consolidated Information Asset Register that identifies information assets, assigned owners, classifications, processing purposes, and data flows.			
8	Management will: • Configure Intune, Defender Device Control or equivalent endpoint protection tooling to block unauthorised removable media by default. • Allow access only to RBFRS-issued encrypted devices and prevent the use of non-approved USB storage.	Medium	Service Operations Manager	30 November 2026

AUDIT OUTCOME OVERVIEW - BUSINESS CONTINUITY

Background: We undertook a review of Business Continuity as part of the approved 2025/26 internal audit plan. The objective was to review the operational business continuity arrangements in place where the Service must deal with situations such as the unavailability of staff or key systems. This included an assessment of the arrangements themselves, as well as the testing and review processes designed to ensure they remain effective.

As a Category 1 responder under the Civil Contingencies Act 2004, the Service is required to maintain plans to ensure it can continue delivering its critical functions during periods of disruption. Business continuity management provides a structured process for identifying essential activities, assessing the impact of their loss, and setting out the steps required to maintain or recover them. Effective arrangements support operational resilience, reduce the likelihood of service interruption, and enable the Service to fulfil its statutory duties.

Over the past year, the Service has taken steps to strengthen its Business Continuity Management System (BCMS). There exists an updated policy and guidance document which outlines roles, responsibilities and ownership across the organisation, and each department and fire station is expected to complete a Business Impact Assessment (BIA) and Business Continuity Plan (BCP) using a standardised template. A Business Continuity Steering Group has been established to oversee the framework, monitor progress and escalate issues to senior management where appropriate. The Service has appointed a dedicated Business Continuity and Resilience Officer to support the ongoing development and strengthening of business continuity arrangements across the organisation.

The Service has also introduced a structured exercising programme, with quarterly themed scenarios, such as loss of site, loss of staff, loss of ICT or loss of equipment, intended to test how well individual plans would operate in practice. Outputs from these exercises are expected to be recorded through a central learning process and used to inform updates to BCPs. These arrangements are supported by wider internal and multi-agency structures, including the Critical Event Management Team and participation in the Thames Valley Local Resilience Forum, which enable coordinated response and recovery during major incidents.

As part of this review, we benchmarked the Service's approach against three comparable clients within the sector and recognised good practice, focusing on the frequency of BCP exercising, the formal identification of critical areas, and whether business continuity training is mandated. The benchmarking summary is provided in Appendix A of this report.

Conclusion: We identified several controls that were well-designed and operating effectively, considering the emerging maturity of the business continuity function. The Service has clear and comprehensive Business Continuity Policy and Guidance documents that set out roles, responsibilities, and governance expectations, and these are readily accessible to staff. Strong oversight is also in place through the Business Continuity Steering Group, Operational Learning and Assurance Board and related governance structures, which provide appropriate challenge, escalation routes, and support for embedding the Business Continuity Management System. The exercising programme is well structured, with quarterly themed scenarios communicated through Siren SharePoint, and we confirmed that guidance for coordinated response is clearly articulated across several key documents. In addition, critical suppliers were broadly consistent with what we would expect for the sector, with continuity considerations evident in all applicable contracts reviewed.

However, we did identify some weaknesses in the current control framework. These include inconsistent completion of BIAs and BCPs and gaps in exercising compliance. We also noted instances where learning from exercises was not reflected in updates to BCPs, and an organisation-wide assessment of critical functions had not yet been completed. These gaps limit the Service's ability to fully assure its resilience arrangements and highlight the need for continued strengthening of the BCMS.

Internal audit opinion:

Audit themes:

We identified the following exceptions, resulting in the agreement of two medium priority management actions:

Supporting BIAs – We reviewed a sample of 10 BCPs from the Business Continuity Schedule Tracker and confirmed that eight had a supporting BIA in place. However, we found that the remaining two did not have one in place at the time of our review despite the Business Continuity Management Policy and Guidance both requiring responsible managers to complete BIAs to identify key tasks and assess the impact of their loss. **(Medium)**

BCP Exercising – From our sample of 10 BCPs, we found that none had completed the required exercises for Q4 at the time of our review. We were informed that the exercising process prior to this quarter was conducted informally, and as a result, no evidence was available to demonstrate that any exercising took place before the introduction of the formal exercising programme. **(Medium)**

We noted the following controls to be well designed and operating effectively:

Policy and Guidance – We reviewed the Business Continuity Management Policy and Guidance and confirmed that both clearly define the key roles, responsibilities, and ownership required for an effective business continuity framework. We also confirmed that the documents have been formally approved by an appropriate SLT member and are readily accessible to staff via the intranet.

Business Continuity Steering Group and Operational Learning and Assurance Board (OLAB) – We reviewed the Terms of Reference (ToR) for the Business Continuity Steering Group and confirmed that it clearly defined the group's responsibility to oversee, support, and advise on the Business Continuity Management System, including escalation routes and links to OLAB. We also confirmed that the ToR were approved in January 2026. Additionally, we reviewed the notes and action log from the group's first meeting, which showed active discussion of continuity culture, resourcing, and compliance, with five actions recorded and assigned to specific owners.

We reviewed the ToR for the Operational Learning and Assurance Board and confirmed that the forum review and evaluate learning captured from activities, including incident monitoring, exercises, and business continuity processes.

Exercising Programme – Through review of the Exercise Event tracker, we confirmed that each quarter has its own risk-type scenario theme including loss of site, loss of staff, loss of ICT and loss of equipment. We also confirmed that these exercise themes were shared with staff via the Siren SharePoint.

Coordinated Response – We reviewed the following documents regarding guidance for coordinated response:

- Critical Event Management Policy
- Draft Critical Event Management Policy
- Duty Officer Guidance
- Operations Support Room Guidance

We confirmed that in each document, guidance was detailed for supporting coordinated response and recovery as well as the duty to share information and cooperate with other responders.

We reviewed an example of a coordinated exercise, Operation Erebus, which took place in October 2025. We confirmed that within the Communication/Engagement Plan, both internal and external stakeholders had been identified as groups to communicate with due to their interest of influence in the operation.

We also reviewed the ToR for the TVLRF Business Continuity Capability Group and confirmed that it included representation from a range of organisations, including Affinity Water, local councils, the NHS, neighbouring Fire and Rescue Services, Ambulance Services and Police.

Critical Suppliers – We were informed that eight suppliers were critical to the business. This included services for mobilising systems, PPE, Thermal Imaging Cameras, and Fire Fighting Foam. We noted that these were in line with critical suppliers that would be expected for the sector. We also confirmed that all applicable contracts for critical suppliers had a BCP included.

Supplier BCPs – We reviewed the list of new suppliers since April 2025 and confirmed that nine suppliers had been contracted during this period. Of the nine contracts, four included a BCP, four did not require one, and the remaining one did not contain a BCP however this was not an issue as it was not identified as a critical supplier (maintenance of water coolers and chillers for staff consumption).

We also reviewed contracts for suppliers identified as critical to the Service. Of these, seven of the eight contracts included either a BCP or alternative continuity provisions. For the remaining supplier, we were informed that a BCP had not been requested as part of the mini competition led by the local County Council on behalf of TVFCS, as this related to Emergency One (UK) and the provision of fire pumping appliances, with the contract and responsibilities held by TVFCS.

We also agreed five **low** priority management actions, details of which can be found within the detailed findings and actions section of this report.

SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

High
Immediate management attention is necessary.

Medium
Timely management attention is necessary.

Low
There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
4	BIAs will be completed for every BCP at the point the plan is created or reviewed.	Medium	Katie Hutton Martyn Doolin	31 August 2026
7	a) BCP exercises will be undertaken, as per the frequency defined in policy. b) All exercises will be included in the learning log once completed. If lessons learned have been identified and have not been included in the learning log or BCP, the rationale behind this will be documented.	Medium	Katie Hutton Martyn Doolin	a) 31 August 2026 b) Complete

APPENDIX A: BENCHMARKING

We completed benchmarking against three comparable clients and recognised best practice to assess the Service's current approach to business continuity management.

The benchmarks focused on the frequency of BCP exercising, the definition of critical areas, and the use of mandatory business continuity training, allowing us to compare the Service's arrangements with those adopted elsewhere which the Service may wish to consider when exercising their own BCPs to increase efficiencies and manage resources effectively.

Benchmark	RBFRS	Client A	Client B	Client C	Best Practice
Exercising of BCPs	Quarterly	Annual desktop exercise, live exercise every 3 years	Strategic and Tactical every six months, Operational annual	2 exercises per year	High criticality BCPs - every 6 months. All other BCPs - annually
Critical areas formally defined	No	Not tested	Yes	Yes	Yes
Mandatory BC Training	Yes	Not tested	Voluntary	Not tested	Yes