DORSET & WILTSHIRE
FIRE AND RESCUE

SWAP
INTERNAL AUDIT SERVICES
Helping Organisations to Succeed

Item 24/57 Appendix A

Dorset & Wiltshire Fire and Rescue Service

Report of Internal Audit Activity

Plan Progress 2024/25 Quarter 3

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Unrestricted

Internal Audit Plan Progress 2024/25 Quarter 3

Contents

The contact at SWAP in connection with this report is:

Dan Newens
Assistant Director
Tel: 020 8142 5030
daniel.newens@swapaudit.co.uk

Internal Audit Plan Progress 2024/25 Quarter 3

Introduction

This report summarises the Internal Audit activity completed for Dorset & Wiltshire Fire and Rescue Service in Quarter 3 2024/25 in line with the Annual Audit Plan approved by the Finance & Audit (F&A) Committee and the Chief Fire Officer in March 2024.

The schedule provided in Appendix 1 contains a list of all Audits agreed in the Annual Audit Plan 2024/25.

We have provided a summary of activity which outlines our assurance opinion and the number and priority of any actions that we made in relation to the Audit work undertaken in Quarter 3. To assist the Committee in its monitoring and scrutiny role, a summary of each audit (objective, risk, controls tested, findings and actions) has also been provided, the content of which has been discussed and agreed with the responsible Director.

The scope for each Audit is agreed in advance with nominated managers. This process intends to focus on the key risks to which that area of the Services activity is exposed and the associated controls which we would expect to be in place to ensure that risk is managed.

The key controls have been assessed against those we would expect to find in place if best practice in relation to the effective management of risk, the delivery of good governance and the attainment of management objectives is to be achieved. Where applicable, selected and targeted testing has been used to support the findings and conclusions reached.

We have performed our work in accordance with the principles of the Institute of Internal Auditors (IIA) International Professional Practice Framework (IPPF) and the Public Sector Internal Audit Standards (PSIAS) in so far as they are applicable to an assignment of this nature and you, our client.

Internal Audit Plan Progress 2024/25 Quarter 3

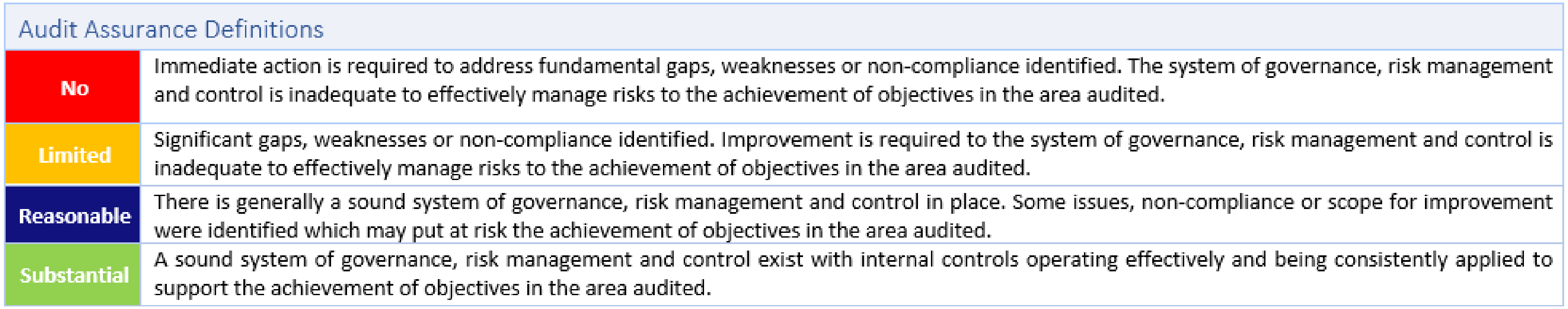
Audit Summary

In Quarter 3 2024/25, the following Audits were completed in accordance with the Audit Plan:

Audit Name	Healthy Organisation Theme	Linked To	Status	Opinion	No of Actions	Priority of Actions		
						1	2	3
Access and Account Management & Control	People & Asset Management Information Management	Strategic Risk 301	Final	Reasonable	2	-	-	2
Operational Risk Information	Corporate Governance Risk Management		Final	Substantial	2	-	-	2

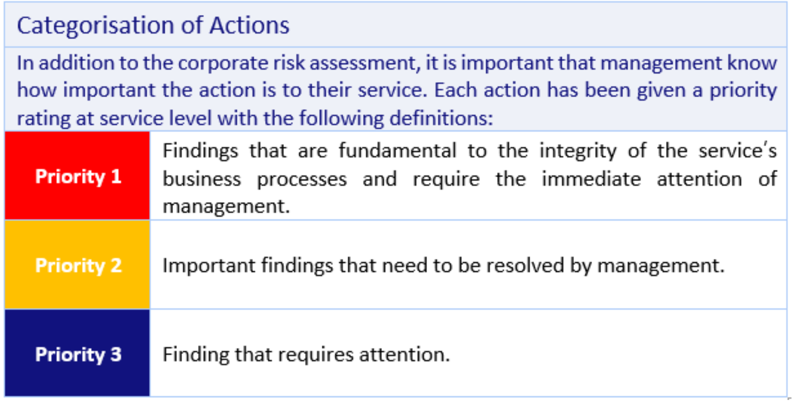
Assurance Definitions

Each completed Audit has been awarded an “Assurance opinion” rating. This opinion takes account of whether the risks material to the achievement of the Services objectives for this area are adequately managed and controlled. The Assurance opinion ratings have been determined in accordance with the Internal Audit “Audit Framework Definitions” as detailed in the below:



Audit Assurance Definitions	
No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance identified. Improvement is required to the system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Reasonable	There is generally a sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Substantial	A sound system of governance, risk management and control exist with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

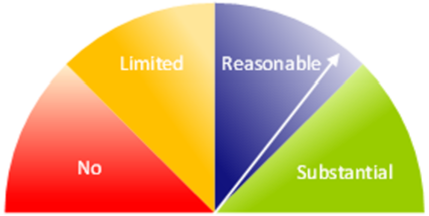
From our work In Quarter 3, we have raised actions which seek to strengthen the Services controls within each Audit area. We highlight those matters of that we believe merit acknowledgement in terms of good practice or undermine the system’s control environment, and which require attention by management. All improvement actions are allocated a priority grading and have been agreed with the management teams in the appropriate area.



Categorisation of Actions	
In addition to the corporate risk assessment, it is important that management know how important the action is to their service. Each action has been given a priority rating at service level with the following definitions:	
Priority 1	Findings that are fundamental to the integrity of the service’s business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management.
Priority 3	Finding that requires attention.

Access and Account Management & Control

Executive Summary

	Assurance Opinion	Management Actions	
	Reasonable (High) - The review highlighted a generally sound system of governance, risk management and control in place. We identified some issues, non-compliance or scope for improvement which may put at risk the achievement of objectives.	Priority 1	0
		Priority 2	0
		Priority 3	2
		Total	**2**

Audit opinion:
Reasonable Assurance

Objective:
To review the controls in place for Account Management to reduce risks of data breaches and malicious access and organisational harm.

Risk reviewed:
Failure to manage user access effectively may result in inappropriate access to data. This will increase the chance of intentional or accidental data breaches, either by users themselves or by malicious actors who have gained control of user accounts.

Access and Account Management & Control

Controls tested:

The following areas of control were covered under the scope of this audit programme:

- An overview of processes for managing IT accounts across the Service infrastructure for software systems owned by departments in the business.
- A review of starters, leavers, and movers within the Service.
- Ensuring that Information Asset Owners responsibilities are clearly defined.
- Ensuring that admin privileges arrangements are in place.
- A review of password security requirements and prompts.
- There is adequate monitoring and assurance provided for all systems.
- A brief review of the current single sign-on project.

It was not possible to test user access permissions as originally intended, see finding 2.

Areas of Good Practice:

- There is a robust policy in place relating to physical information management and information risk management, clearly defining roles and responsibilities.
- The reporting mechanism for alerting appropriate bodies in the incident of a data breach is clear and easy to follow and is in keeping with statutory guidance on how to manage cyber threats as per the National Fire Chiefs Council and the Information Commissioners Office.
- The implementation of the Password Policy Manager has provided an effective way of ensuring that passwords are robust and reduces the risk of unauthorised access. By rolling out a service-wide renewal of passwords to flow in accordance with the new Password Policy Manager, the Service can now ensure that the risk of password cloning and scanning for commonly used passwords can be reduced with complexity requirements in keeping with advice provided by the National Cyber Security Centre.
- The Service is implementing a single sign-on authentication process across the Service which allows users to access multiple systems and Microsoft applications using their unique login credentials through Microsoft 365. This project seeks to add additional controls for both Information Asset Owners and the ICT team reducing the risk of malicious harm.

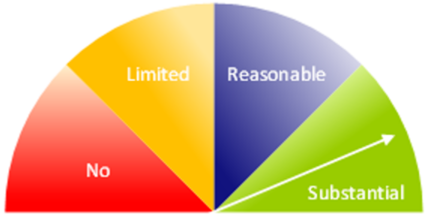
Summary of Actions:

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
The Delete User Procedure is clear and easy to follow and has recently been updated. It provides clear guidance for officers completing the four-stage task of deleting users. There are robust auditing processes in place that act as a secondary line of defence as part of the four-stage closure of accounts as an oversight mechanism. We tested 168 Service leavers against the current users contained within Active Directory's Active OU Group. In this testing, we identified three leavers who were still showing as having active user access accounts. When reviewing the three user accounts, two accounts were disabled immediately during the discussion and moved to the Leavers OU Group, and the ICT Team Leaders identified one user account whose ICT Helpdesk notes advised they had completed the deletion process, but they had not been moved into the Leavers OU group for closure review or audit. The ICT Team Leaders advised that a 6-monthly report compiled by the Networking and Infrastructure Team for a list of all active OU Users would be beneficial, so they can ensure moving forward that all users who are marked as leavers are removed from active OU groups and moved into the Leavers OU Groups where they can be appropriately monitored.	Produce and review a 6-monthly report of active users from the Active OU group by Networking and Infrastructure to ensure that all users marked as "Leavers" are identified and monitored.	A six monthly report will be provided by the Networking and Infrastructure Team to enable a comparison of active users and leavers, providing assurance that any gaps are addressed.	Head of ICT 31 October 2024 Complete	3
The New Starter Creation guide is very comprehensive. It is a detailed "How To" guide for Administrators to set up new users for Microsoft 365.	The Information Governance Manager will produce an access checklist for Information Asset	A template for will be developed for relevant managers and this will be monitored for completion of this via	Information Governance Manager	3

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
However, we were unable to carry out testing of employee's access permissions due to the required permissions not being documented. There is no access/ permission matrix in place to assign permissions to accounts based on roles and setting up permissions is solely reliant on communication from Managers or Team Leaders. Therefore, without a matrix or documented requirement of permissions to test against, staff permissions could not be tested. It is recognised that many users carry out a number of different roles across the service, and therefore a matrix may be difficult to establish. However, basic administrator rights for each service and multi-role users' access should be documented.	Owners (IAOs) to ensure that starters and organisational movers access permissions are created without delays, and officers' access can be tested against for audit purposes.	the Digital, Data and Technology Board.	30 April 2025	🟦

Operational Risk Information

Executive Summary



Assurance Opinion	Management Actions	
A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	Priority 1	0
	Priority 2	0
	Priority 3	2
	Total	**2**

Audit Opinion:
Substantial Assurance

Objectives:
To provide assurance there are adequate controls and oversight is in place to ensure operational staff have the correct and most up to date information needed, which is accessible as required, to ensure a safe response.

Risk Reviewed:
The public, operational staff and/or the environment suffer from harm because up to date and complete operational risk information is not available to operational staff.

Operational Risk Information

Controls Tested:

We reviewed the adequacy and effectiveness of the following controls established for acquiring and disseminating operational risk information implemented and delivered through the Operational Risk Team proof-of-concept trial and future agreed arrangements:

- Adequate procedures, knowledge and access exists to ensure operational risk information is identified, classified, and recorded.
- The content of operational risk information is reviewed and tested to ensure its accuracy.
- Operational risk information is available and accessible when required.

Areas of Good Practice:

The following key strengths were identified during our review:

- Adoption of the Chief Fire Officers Association (CFOA) model; Provision of Risk Information System (PORIS) to capture, evaluate and treat operational risk.
- Operational risk information captured by the Community Fire Risk Management Information System (CFRMIS) and shared via the Risk Information Sharing Portal (RISP) to appliance based Mobile Data Terminals (MDT's) and Risk Information Tablets (RITs).
- CFRMIS does not currently link and upload to RISP (used to publish to MDTs) and is therefore a manual process but is expected to be addressed in the next six months by implementing the new Ops Intel Package with the ability to link and auto publish to the MDTs.
- Monthly report sent to Operational District Commanders, Group and Area Managers highlighting overdue inspections, a summary of risk reviews completed and published on the MDTs in the month, the number of reviews due in the following six-month period and the number of risk reviews undertaken for temporary events.
- Good processes in place for sharing operational risk information internally and cross border (inward and outward) to neighbouring fire and rescue services with documented MOUs either planned or in place for non-Network Fire Service Partnership neighbours.
- The Draft Operational Risk Quality Assurance and Auditing document outlines the proposed QA and Audit processes and a step-by-step guide for completion. The Operational Risk team will be implementing the processes, along with other minor suggestions made during this review as the new structure embeds.

Summary of Actions:

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
RE14 – Identification and Management of Operational Risk Information sets out the arrangements for identifying, communicating, and managing operational risk information within the Service. The last review of RE14 was November 2023 (i.e. reflecting the arrangements prior to the revised arrangements being approved) and should, along with other related procedures such as *PR18 – Public Event Safety*, be updated to reflect the revised structure for operational risk.	Review and update *RE14 – Identification and Management of Operational Risk Information* and other related procedures to reflect the revised operational risk structure.	RE14 is constantly updated as/when processes are changed. It will be updated in early 2025, once the new Operational Risk team have been trained and embedded into ways of working.	Station Manager Risk & Resilience 31 March 2025	3
For loss of MDTs, the Service Support Business Continuity plan is instigated. The Business Continuity Team are creating 'loss of software systems' documents to support department business continuity arrangements for systems loss. Alternate arrangements exist in case of loss of MDT's and other systems including mobile phone access to RISP and SharePoint and if there is a total loss, fire and rescue crews defaulting to on-site dynamic risk assessments when on scene. It is advisable to periodically test the effectiveness of the business continuity arrangements.	When the "loss of software systems" Business Continuity plan is drafted the opportunity should be taken to test the plan in the event of loss of access to the MDTs.	The loss of software systems are part of each departments Business Continuity Plans and are reviewed regularly and exercised as part of the exercise procedure in line with the business continuity plan of work. We exercised loss of software as part of the National Power Outage exercise on 15th October 2024. We will also continue to work on these plans as part of business as usual work.	Station Manager Risk & Resilience Complete	3

Appendix 1 – 2024/25 Audit Plan and Performance

Audit Name	Healthy Organisation Theme	Linked To	Status	Opinion	No of Actions	Actions		
						1	2	3
Social Media Arrangements	Corporate Governance		Final	Reasonable	3	-	3	-
MTFP & Financial Resilience	Financial Management	Strategic Risk 0006	Final	Substantial	0	-	-	-
Data, Digital and Technology Strategy	Information Management Corporate Governance	Strategic Risk 301	Final	Substantial	0	-	-	-
Site Security	People & Asset Management		Final	Reasonable	5	-	4	1
Access and Account Management & Control	People & Asset Management Information Management	Strategic Risk 301	Final	Reasonable	2	-	-	2
Operational Risk Information	Corporate Governance Risk Management		Final	Substantial	2	-	-	2
Planned and Reactive Fleet Maintenance	People and Asset Management Procurement and Commissioning		Not Started					
Workforce Planning Arrangements	People and Asset Management		Not Started					
Follow Ups	All	All	-					

The performance results for progress against the internal audit plan for Quarter 3 of the 2024/25 Internal Audit Plan are as follows:

Performance Target	Average Performance	
	% of the Annual Plan	Number of Assignments
Audit Plan – Percentage Progress		
Final, Draft, Discussion, Removed	75%	6
In progress, Ongoing	0%	0
Not yet started	25%	2
	100%	8

The completion of the plan is currently on target.