DORSET & WILTSHIRE FIRE AND RESCUE

SWAP INTERNAL AUDIT SERVICES
Helping Organisations to Succeed

Item 24/43 Appendix A

Dorset & Wiltshire Fire and Rescue Service

Report of Internal Audit Activity

Plan Progress 2024/25 Quarter 2

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Internal Audit Plan Progress 2024/25 Quarter 2

Contents

The contacts at SWAP in connection with this report are:

David Hill
Chief Executive
Tel: 020 8142 5030
david.hill@swapaudit.co.uk

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

Internal Audit Plan Progress 2024/25 Quarter 2

Introduction

This report summarises the Internal Audit activity completed for Dorset & Wiltshire Fire and Rescue Service in Quarter 2 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 2. 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 2

Audit Summary

In Quarter 2 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
Digital, Data and Technology Strategy	Information Management Corporate Governance	Strategic Risk 301	Final	Substantial	0	-	-	-
Site Security	People & Assets Management		Final	Reasonable	5	-	4	1

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:

Assurance Definitions	
None	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 were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
Reasonable	There is a generally 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 exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

From our work in Quarter 2, 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.

Digital, Data and Technology Strategy

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	0
	Total	**0**

Audit Opinion:
Substantial Assurance

Objectives:
To review the Data, Digital and Technology Strategy (DDTS) to ensure it aligns with corporate aims and objectives and appropriate and realistic to deliver the operational and project requirements of the Service.

Risk:
The Data, Digital and Technology Strategy does not align with organisational objectives and risks and inadequately resourced leading to reputational, cyber security, and financial risks.

Digital, Data and Technology Strategy

Controls Tested:

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

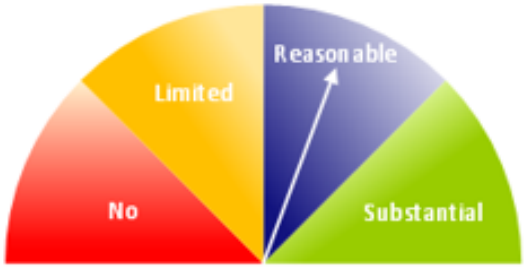
- The Strategy aligns with corporate aims and objectives.
- The Strategy is fit for purpose and aligned with organisational and project objectives and risks.
- Benchmarking of the Strategy was carried out to identify any gaps and additional areas of practice.
- The Strategy is adequately resourced and effective succession planning is undertaken.

Areas of Good Practice:

- There was alignment between the Strategy, Strategic Assessment of Risk, and the Community Safety Plan.
- There is a process in place to deliver the DDTS through service delivery plans and linking risks to organisational and project objectives.
- Benchmarking of the Strategy found that it was well positioned, clear, concise, and included all of the areas expected.
- The Strategy was adequately resourced with annual service area and corporate succession planning initiatives in place.

Site Security

Executive Summary



Assurance Opinion	Management Actions	
There is a generally 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.	Priority 1	0
	Priority 2	4
	Priority 3	1
	Total	5

Audit Opinion:
Reasonable Assurance

Objectives:
To review the quality and effectiveness of the management controls in place to ensure site security, including the escalation and communication when the national security threat is raised.

Risk:
There are ineffective site security arrangements and management controls in place to protect assets and personnel leading to reputational, safety, and financial risks

Site Security

Controls Tested:

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

- There are clear policies and procedures in place which outline site security requirements and the thresholds of implementation according to the national threat level.
- Training is provided to staff to ensure information and implementation is consistent and relevant.
- Site security and management controls are implemented as per the policy requirements and staff are aware of their responsibilities.
- Site security expectations and roles and responsibilities are included in contracts and monitored.
- There are clear lines of communication internally and externally to raise awareness of site security.
- Site security forms part of the business continuity planning and testing.
- There is monitoring and reporting across all sites to ensure corporate oversight.

Areas of Good Practice:

- All sites are designed to secure themselves through self-locking doors and there is ongoing improvements and maintenance to site security arrangements.
- Site security inspections take place biannually and on an ad hoc basis. These are monitored by the Resilience Team monthly, and any issues are raised with the relevant staff members.
- There is a process in place to report maintenance or any issues via a Work Service Request.
- Recruitment involves the completion of DBS checks.
- ID cards are required to access DWFRS sites and restricted where required.
- There is an up-to-date Management of Contractor Procedure which outlines DWFRS's key roles and responsibilities.
- Contractors are made aware/ reminded of their site security roles and responsibilities through the annual Health & Safety update.
- There are adequate processes in place to communicate awareness of site security internally and externally.
- There are adequate controls in place for testing the Business Continuity Plans and incident response plans which clearly set out the thresholds of implementation according to the national threat level.
- Benchmarking found that there is generally good awareness of site security arrangements.

Summary of Actions:

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
Site security training is available to staff, however, completion is not mandatory, monitored or reported. In addition, refresher training is not a requirement and does not form business as usual. The Access Control Procedure (ACP) states that staff have a 'legal duty to comply with this policy through a program of physical security awareness training' and that 'It is accepted that some members of staff will require varying degrees of security training dependent on specific roles and responsibilities', however, we found that: • The current program of physical security awareness training available to staff consists of 'general training' through the induction process. However, while site security is covered on the induction checklist, which is signed and agreed, the ACP is not included on the list. • A site security e-learning module is available to all staff. However, this is not compulsory, required to be refreshed periodically, and completion is not monitored.	• To review the site security training available to staff and ensure this is sufficient, compulsory, requires refreshing periodically, and completion is monitored. • To create a training matrix outlining the varying degrees of security training required for specific roles and responsibilities. • To include the ACP on the induction checklist. • Once the above elements have been discussed and agreed, the ACP should be updated to reflect the requirements.	A review of security training to take place and will be overseen by the new Protective Security Group. The ACP will be reviewed and either have a new section added or a supporting information document created that will cover the induction. This will include a matrix covering roles and responsibilities.	Group Manager Resilience and Risk 15th November 2024	2

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
• There is not a training matrix outlining the varying degrees of security training dependent on specific roles and responsibilities. It is recognised that a new Protective Security Group is being formed which will review the training provided to staff and ensure a joined-up approach across the service from September 2024.				
It is recognised that there is a weekly process in place to manage leaver's ID cards. Sample testing found that in all those reviewed between April, May, and June 2024, all leavers ID cards had been deactivated. However, a full reconciliation of the system has not been carried out to identify any leavers that have not been deactivated or inactive users.	To carry out a full system reconciliation at a frequency deemed suitable for the Service.	Although the audit has revealed that all leavers over the last three months have been deactivated, the Service will undertake a full reconciliation of the system, to ensure that none have been missed over the previous twelve months.	Head of Assets 31st October 2024	3
Contractors requiring site access are issued ID cards, which are managed by the Estates Team. However, contractor ID cards have not been monitored regularly. Currently, the Team are reviewing the Access Control System and contacting contractors to identify those who are still active, those who have departed, and any new starters. There is a risk that contractors that no longer	To complete the ongoing review of contractors and implement a process to monitor contractor ID cards at a frequency deemed suitable for the Service.	Our internal procedure will be updated to include this process below: • Add to the list of contractors who have ID cards a list of their employee names. • Complete an annual review with the contractors to check the lists are up to date.	Head of Assets 15th November 2024	2

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
work for DWFRS, or contractor's staff who have left the company, may still have unauthorised access to DWFRS sites, potentially compromising security.				
It was explained during the audit that contractors are required to have DBS checks in place to work at DWFRS sites. During the procurement process, a Standard Selection Questionnaire (SSQ) is sent to each contractor bidding on a contract who must select 'yes' or 'no' to the following statement: Please self-certify that you have in place processes to ensure that any personnel who may be employed to undertake work pursuant to and in support of this Contract can be DBS checked? By selecting 'no' that contractor will not be processed any further. However, the wording: 'can be DBS checked' suggests it is not mandatory for contractors to be DBS checked. The SSQ does not specify that DBS checks are a requirement, who is responsible for carrying them out or the level of check required. Assurance is provided by contractors that staff are DBS checked via the SSQ statement at the start of the contract and on contract renewal. DWFRS do not request copies of DBS certificates. By not requesting copies of DBS certificates, the Service risks compromising its security protocols, increasing its vulnerability	• To amend the wording of the SSQ to reflect that DBS checks are a requirement. • To determine, document, and implement processes to monitor and manage contractors DBS checks, at a frequency deemed suitable for the Service, and determine who within DWFRS will be responsible for this oversight.	We have over 300 contractors with multiple employees; in order to review all DBS checks for contractors coming onto sites, we would need a considerable increase in resources. This could create a risk as without the resources to adequately check all contractors coming on to site, it leaves us with the responsibility to ensure everyone is DBS checked, and we would be unable to fulfil a commitment to checking all contractors DBSs. The risk should be with the contractor, as it is, to assure us that they complete DBS checks. The risk is we could have contractors on site that have not been DBS checked. We agree that the wording of the SSQ should be changed but it should state that they will certify that all of their staff coming onto DWFRS sites have been DBS checked and that there are no adverse results.	Head of Assets 30th September 2024	2

Findings & Risk	Action	Management Response	Officer Responsible/ Timescale	Rec Priority
to potential threats, reduced trust and accountability, potentially affecting the overall integrity of site security measures. Additionally, ID cards are issued to contractors without complete assurance that valid DBS checks are in place, despite this being the process for staff.				
There is an up-to-date ACP which outlines the key roles, responsibilities, and features of site security. However, it does not outline how site security should be monitored and reported corporately. While it was evident that team meetings are discussing site security, Officers confirmed that site security has not been reported on corporately in the past. Going forward, site security will be included on the quarterly service delivery report and a Protective Security Group is being formed in September 2024.	• To update the ACP with the corporate monitoring and reporting arrangements. • To ensure the Protective Security Group includes representatives from across the Service including Estates and Assets, and a Terms of Reference is produced outlining the members, roles and responsibilities, meeting frequency, reporting and escalation arrangements, and aims and objectives.	Quarterly security reports will be conducted as part of the Service Delivery Team quarterly updates This will include reviewing and reporting on all reported security incidents. The Protective Security Group will be implemented within Q2 of 2024 with representatives from across the service and a Terms of Reference will be produced. The ACP will be updated to include corporate monitoring and reporting arrangements.	Group Manager Resilience & Risk 29th November 2024	2

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	1	-	-	1
Medium Term Financial Plan (MTFP) & Financial Resilience	Financial Management	Strategic Risk 0006	Final	Substantial	1	-	-	1
Data, Digital and Technology Strategy	Information Management Corporate Governance	Strategic Risk 301	Final	Substantial	0	-	-	-
Site Security	People & Assets Management		Final	Reasonable	5	-	4	1
Access and Account Management & Control	People & Assets Management	Strategic Risk 301	Not Started					
Operational Risk Information	Corporate Governance Risk Management		Not Started					
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 2 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	50%	4
In progress, Ongoing	0%	0
Not yet started	50%	4
	100%	8

Completion of the plan is currently on target.