DORSET & WILTSHIRE FIRE AND RESCUE

SWAP INTERNAL AUDIT SERVICES
Helping Organisations to Succeed

Item 26/48 Appendix A

Dorset & Wiltshire Fire and Rescue Service

Report of Internal Audit Activity

Plan Progress 2026/27 Quarter 3

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Unrestricted

Internal Audit Plan Progress 2026/27 Quarter 3

Contents

The contact at SWAP in connection with this report is:

Dan Newens
Director of Specialist and Client Services
Tel: 020 8142 5030
daniel.newens@swapaudit.co.uk

Jodie Bromell
Assistant Director
Tel: 020 8142 5030
jodie.bromell@swapaudit.co.uk

Introduction	Page 2
Audit Summary	Page 3
Assurance Definitions	Page 4
Cyber Security Audit Detail	Page 5-14
Health and Wellbeing Arrangements Audit Detail	Page 15-19
Appendix 1 – 2026/27 Audit Plan and Performance	Page 20-21

Internal Audit Plan Progress 2026/27 Quarter 3

Introduction

This report summarises the Internal Audit activity completed for Dorset & Wiltshire Fire and Rescue Service in Quarter 3 2026/27 in line with the Annual Audit Plan approved by the Finance & Audit (F&A) Committee and the Chief Fire Officer in February 2026.

The schedule provided in Appendix 1 contains a list of all Audits agreed in the Annual Audit Plan 2026/27.

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 Service's 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) Global Internal Audit Standards (GIAS) and the UK Public Sector Application Note and the CIPFA Code of Practice for the Governance of Internal Audit in UK Local Government in so far as they are applicable to an assignment of this nature and you, our client.

Internal Audit Plan Progress 2026/27 Quarter 3

Audit Summary

In Quarter 3 2026/27, 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
Cyber Security	Information Management	Strategic Risk 301 HMICFRS Efficiency Pillar Priority 4	Final	Reasonable	9	-	7	2
Health and Wellbeing Arrangements	People and Asset Management	Strategic Risk 598 HMICFRS People Pillar Priority 5	Final	Reasonable	4	-	1	3

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 Service's 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 we have raised actions which seek to strengthen the Service's controls within each Audit area. We highlight those matters 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.

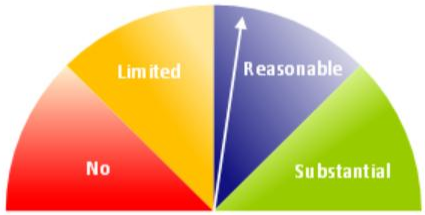
Categorisation of Actions	
In addition to the corporate risk assessment, it is important that management know how important the action is to their service. Each action has been given a priority rating at service level with the following definitions:	
Priority 1	Findings that are fundamental to the integrity 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.

Cyber Security

Audit Objective

Provide assurance over the arrangements in place at DWFRS to understand, assess and manage cybersecurity risks and protect IT systems and networks from cybersecurity threats.

Executive Summary



Assurance Opinion

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 in the area audited.

Management Actions

Priority 1	0
Priority 2	7
Priority 3	2
Total	9

Organisational Risk Assessment — Medium

Our audit work includes areas that we consider have a medium organisational risk and potential impact.
The key audit conclusions and resulting outcomes warrant further discussion and attention at senior management level.

Key Conclusions

The automated patching process for server ASR-206 could not be confirmed as operating effectively, with the 2026 IT Health Check identifying 49 servers with missing security updates compared with 4 in 2025. This increases the risk that known vulnerabilities remain unremediated, potentially exposing DWFRS systems to compromise or service disruption.

The cybersecurity policy framework is not sufficiently current or comprehensive, with key policies and supporting procedures either outdated, incomplete, or not evidenced as being regularly reviewed and approved. This increases the risk of inconsistent application of cybersecurity requirements and limits assurance that controls remain aligned with DWFRS's current cyber risks and operational environment.

Audit Scope

The audit was a focused assurance review aligned to CAF Objective A – Managing Security Risk and Objective B – Protecting Against Cyber Attack. It covered:

- Cybersecurity governance, policies, risk management, roles and reporting;
- Identification of important systems, information and third-party

	The DWFRS SD-WAN firewall policy and external security assessment identified overly permissive firewall rules, including broad source and destination ranges, unrestricted services, temporary rules and legacy protocols such as FTP/TFTP. This increases the risk of unnecessary or unauthorised network access and limits assurance that firewall controls are appropriately restricted and securely maintained.
	User access could not be confirmed as appropriate or authorised, as roles and associated permissions were not clearly defined and evidence of consistent access administration was not available. This increases the risk of inappropriate or excessive access remaining in place and limits assurance that systems, data and services are protected from unauthorised access or change.
	DWFRS has established a broad suite of cyber-related policies and procedures covering information security, asset management, systems administration, incident response, data breaches and change management. However, note the finding relating to their upkeep.

dependencies, including one key ICT supplier;

- User and privileged access;
- Vulnerability and patch management;
- Secure configuration and network protection; and
- Backup arrangements, backup protection and restoration testing (high-level).

Other Relevant Information

The review did not assess every element of CAF Objectives A and B. Testing focused on selected important systems and network areas, and the backup and restore work did not constitute a full Data Recovery Review.

Finding 1.	Action
Possible Automated Server patching failure for ASR-206 Testing identified a potential failure in the automated patching process for server ASR-206, indicating that security updates may not have been applied through the standard managed process. This creates uncertainty over whether the server is being maintained in line with defined patching requirements and weakens assurance that known vulnerabilities are being addressed promptly. Rather than improving from the 2025 position (4 affected servers), the 2026 ITHC identified 49 servers with missing security updates, suggesting patch management remains a significant control weakness across the server estate. Where automated deployment does not operate as intended, there is an increased risk that the affected infrastructure remains exposed to unremediated security flaws, increasing the likelihood of compromise, service disruption, or broader impact to connected systems within the DWFRS environment.	1.Investigate the automated patching failure affecting ASR-206 and confirm whether the required security updates were applied. 2. Remediate any missing updates across the server estate, prioritising affected and exposed systems. 3. Validate patch deployment controls to identify why automated patching did not complete as expected and correct the underlying cause. 4. Strengthen monitoring and exception handling so patch failures are detected, escalated, and resolved promptly. **Management Response** Agreed. This will be picked up as part of ITHC remediation work, which is already in progress.

Priority	2	**SWAP Reference**	AP#10779
Responsible Officer		Head of ICT	
Timescale		16/01/2027	

Finding 2.	Action
Cybersecurity Related Policies need updating and supplementing The review identified that, although DWFRS has a broad suite of cybersecurity-related policies and procedures, elements of the framework require updating and greater consistency. Of the eight documents reviewed, specific issues included: • the ICT Change Management Procedure reached its stated review date of 1 October 2026 during the audit and contains duplicated wording and inconsistencies within the emergency change process; • the Information Security Management Procedure, despite being recently updated, contains a number of older technical requirements and references which should be reviewed to confirm that they remain appropriate to the current IT environment; • the CyberAttack Grab Sheet requires review of some of its contact, reporting and technical response instructions to ensure staff are provided with clear and current guidance during a cyber incident; • the Information Security Incident flowchart lacks clear document-control information and requires clarification around incident classification and escalation routes; • the Physical Information Security procedure and Systems Guidance contain inconsistent access-review frequencies, with reviews described variously as regular, six-monthly or annual; and • approval evidence is inconsistent across the suite, with some documents identifying approvers while others only identify an owner, author or published status. The review also identified areas where requirements are currently dispersed across the existing documentation rather than supported by a clearly defined end-to-end process. These include identity and access management, vulnerability management, security monitoring and logging, supplier cybersecurity assurance and secure configuration. As a result, while the existing documents provide broad coverage of cybersecurity requirements, the framework is not yet fully current, consistent and complete, increasing the risk that cybersecurity requirements are interpreted or applied inconsistently.	1. Refresh the cybersecurity policy framework so core policies and supporting procedures are current, complete, and aligned to the organisation's operating environment and cyber risk profile. 2. Establish a formal review and approval cycle with defined ownership to ensure documents are periodically reassessed, updated, and reissued where required. 3. Map related policies and procedures to identify and resolve inconsistencies, gaps, and overlaps so guidance is coherent across the control framework. 4. Communicate updated requirements to relevant staff and service areas, supported by training or awareness activity to promote consistent application. 5. Maintain evidence of review, approval, and version control to support ongoing governance and assurance. **Management Response** Agreed.

Priority	2	**SWAP Reference**	AP#10766
Responsible Officer		Head of ICT and Head of Information Governance and Cyber Security	
Timescale		16.10.2027	

Finding 3.	Action
Lack of Confirmed Cybersecurity roles, responsibilities and accountability which are clearly defined and assigned The organisation can demonstrate that cybersecurity responsibilities exist; however, we are unable to conclude that cybersecurity roles, responsibilities and accountability are fully or clearly defined until a formal Cybersecurity Governance Framework or accountability matrix is introduced.	1. Establish a formal cybersecurity governance framework that clearly defines roles, responsibilities, and accountability across the organisation. 2. Assign ownership for key cybersecurity activities, document the accountability structure, and obtain management approval. 3. Communicate the framework to relevant personnel and review it periodically to keep responsibilities current. **Management Response** Agreed.

Priority	2	**SWAP Reference**	AP#10768
Responsible Officer		Head of Information Governance and Cyber Security	
Timescale		16.10.2027	

Finding 4.	Action
Network Security Controls and Firewall Rule Management Require Strengthening DWFRS has implemented network protection controls, including separate network zones, dedicated firewall infrastructure, DMZ arrangements and SD-WAN connectivity. However, the evidence available did not provide up-to-date assurance over the ongoing operation and review of these controls. The most recent firewall/network access review available for audit was the July 2026 PSN CoCo assessment, and evidence was not available to confirm whether the issues identified had subsequently been addressed. In addition, the July 2026 assessment identified specific weaknesses within the Hub1 firewall rules, including broad source or destination access, excessive permitted services, unencrypted or legacy protocols and temporary rules. This indicates that some network access was broader than necessary at the time of that assessment.	1. Confirm the current status of the issues identified in the July 2026 PSN CoCo assessment and address any that remain outstanding. 2. Review and tighten firewall rules where access is broader than necessary, including broad source/destination access, excessive permitted services, temporary rules and unencrypted or legacy protocols. 3. Establish a regular documented review of firewall and network access rules to confirm that access remains appropriate and unnecessary or obsolete rules are removed. 4. Retain evidence of reviews and remediation undertaken so that the current status of identified network security issues can be demonstrated. **Management Response** Agreed. This will be picked up as part of ITHC remediation work, which is already in progress.
	Priority 2 — **SWAP Reference** AP#10796
	Responsible Officer Head of ICT
	Timescale 16.01.2027

Finding 5.	Action
Backup Arrangements and Protection Controls Not Yet Fully Established DWFRS is renewing its backup arrangements following the implementation of new hardware and the Veeam solution. While operational evidence demonstrated that backups are being performed, the Backup Policy/Procedure and associated backup schedule were still under development and were not available during the audit. Consequently, we could not fully confirm that all important systems and data are covered by formally documented backup arrangements or that backups are being performed in accordance with an approved frequency and schedule. In addition, due to the ongoing renewal of the backup infrastructure, current configuration evidence was not available to confirm that planned protection controls, including immutable repositories, multi-factor authentication (MFA) and encryption, had been fully implemented and were operating as intended.	1. Complete and approve the Backup Policy/Procedure and backup schedule for the new environment, ensuring that all important systems and data are covered and that backup frequency, retention and recovery requirements are clearly defined. 2. Complete implementation of the planned backup protection controls, including immutable repositories, MFA and encryption, and verify that these controls are operating as intended. 3. Retain evidence that backups are completed and reviewed in accordance with the approved arrangements, together with configuration evidence demonstrating that the required protection controls remain enabled and effective. **Management Response** Agreed. This work is already in progress as part of our back up replacement project.

Priority	2	**SWAP Reference**	AP#10798
Responsible Officer		Head of ICT	
Timescale		16.01.2027	

Finding 6.	Action			
Restoration Testing Not Yet Fully Implemented DWFRS is transitioning to the new Veeam backup environment, including implementation of SureBackup. At the time of the audit, restoration testing had not yet become fully operational; therefore, evidence of completed restoration tests, successful restoration outcomes and follow-up of identified issues was not available.	1. Complete the transition to the new backup environment and fully deploy restoration testing capabilities. 2. Establish a recurring process to document test execution, confirm successful recovery results, and track remediation of any issues identified during testing. **Management Response** Agreed. This work is already in progress as part of our back up replacement project.			
	Priority	2	**SWAP Reference**	AP#10800
	Responsible Officer		Head of ICT	
	Timescale		16.01.2027	

Finding 7.	Action			
Unable to evidence that Privileged access is appropriate, authorised, or reviewed DWFRS provided evidence of privileged-access administration through the ManageEngine Ticket #4865, which recorded a request for WH to receive administrator access to SharePoint. The ManageEngine Ticket #4865 demonstrated that the request for WH's SharePoint administrator access was recorded and traceable. However, the evidence provided did not identify the privileged permissions granted, the business or role-based requirement for that level of access, or the approval showing that an appropriately authorised officer had agreed the access before it was granted. Consequently, for this sample, we could not confirm that the level of privileged access granted was appropriate to WH's role and formally authorised.	1. Maintain a complete inventory of privileged access for each user, covering all in-scope systems and entitlements. 2. Require independent verification that all privileged access has been removed before closing the case. 3. Retain formal approval of the review and remediation outcome to evidence proper authorisation. 4. Periodically test the process to ensure privileged access reviews are complete, authorised, and fully documented. **Management Response** Agreed			
	Priority	2	**SWAP Reference**	AP#10812
	Responsible Officer		Head of Information Governance and Cyber Security	
	Timescale		16.04.2027	

Finding 8.	Action
Unable to evidence how often risks are reviewed or how they are monitored and escalated Cybersecurity risks are recorded, but the review process is not sufficiently evidenced to demonstrate how regularly those risks are reconsidered, whether changes in exposure are identified promptly, or how significant issues and related actions are tracked through to resolution. The lack of clear records of monitoring, challenge, and escalation creates uncertainty over whether emerging threats, control weaknesses, or overdue improvement activity are being brought to the attention of the appropriate governance forum in a timely way. Within cyber risk management, this represents a core oversight gap that may limit the organisation's ability to respond effectively to changes in risk across its systems, networks, and key dependencies.	1. Establish a formal cyber risk review cadence with documented evidence of each review, including risk changes, control issues, and follow-up actions. 2. Define clear escalation criteria and maintain an action tracker to monitor remediation through closure. 3. Require governance forum reporting on overdue items and significant changes in exposure to ensure timely challenge and oversight. **Management Response** Agreed. This piece of work had already been identified as an area to strengthen.

Priority	3	**SWAP Reference**	AP#10810
Responsible Officer		Head of Information Governance and Cyber Security	
Timescale		16.01.2027	

Finding 9.	Action
Unable to confirm that user access is appropriate, authorised, or administered We were unable to evidence that user access is appropriately authorised and administered, as the roles are not clearly defined and we were unable to evidence the permissions for each role. As a result, it could not be confirmed that access rights are appropriate to role requirements or that account changes and removals are consistently administered when no longer needed. This creates a gap in a core cybersecurity control, increasing the risk of inappropriate or excessive access remaining in place, including for users whose responsibilities have changed or ended. In the context of important systems and network areas, the lack of demonstrable control weakens assurance over the protection of systems, data, and services from unauthorised use or change.	1. Define and document role-based access requirements for all relevant systems and network areas, including expected permissions for each role. 2. Review existing user access to confirm alignment with approved role requirements, and remove or adjust any inappropriate or excessive access. 3. Implement a formal process for approving, updating, and removing access when users change roles or leave the business, with evidence retained for review. 4. Assign clear ownership for access administration and perform regular reconciliations to verify account changes and removals are completed consistently. 5. Introduce periodic management review of user access to provide ongoing assurance that access remains appropriate and authorised. **Management Response** Agreed. This piece of work had already been identified as an area to strengthen and a project is about to start to address this.

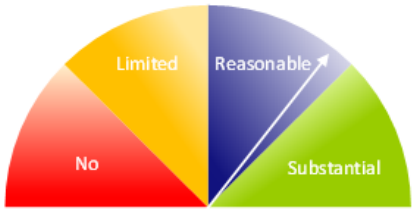
Priority	3	**SWAP Reference**	AP#10811
Responsible Officer		Head of Information Governance and Cyber Security	
Timescale		16.10.2027	

Health and Wellbeing Arrangements

Audit Objective

To provide assurance that the Service has appropriate measures in place to support the health and wellbeing of its staff, with a particular focus on resources and initiatives addressing the primary causes of long-term sickness absence.

Executive Summary



Assurance Opinion

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 in the area audited.

Management Actions

Priority 1	0
Priority 2	1
Priority 3	3
Total	4

Organisational Risk Assessment — Low

Our audit work includes areas that we consider have a low organisational risk and potential impact.

We believe the key audit conclusions and any resulting outcomes still merit attention but could be addressed by service management in their area of responsibility.

Key Conclusions

Whilst annual reviews of wellbeing resources are now being introduced, there is no formal framework to ensure reviews are consistently informed by sickness absence trends and staff feedback. Strengthening the review process would help ensure wellbeing resources remain aligned to workforce needs and the primary causes of sickness absence.

Recent employment legislation has not yet been reflected within the Attendance Management Procedure and supporting guidance.

The Service has not formally reviewed whether existing wellbeing service delivery arrangements, referral routes and appointment availability remain suitable for all staff groups, particularly on-call employees.

Audit Scope

The scope of the audit covered the adequacy and effectiveness of the following controls:

- Attendance management policies, procedures and guidance are up-to-date and provide managers with clear direction on their responsibilities and the actions required to manage attendance effectively;
- Health and wellbeing resources (for Musculoskeletal and Mental Health) are sufficient and aligned with Service strategic objectives and the identified needs of staff;
- Appropriate monitoring arrangements are in place to assess compliance with attendance management procedures, the

	The process for reporting and escalating barriers to wellbeing support has not been formally documented or communicated to staff.	effectiveness of health and wellbeing initiatives, and the performance of contracted wellbeing services; • Health and wellbeing resources (for Musculoskeletal and Mental Health) are effectively communicated and promoted to all staff across the Service, taking account of different roles, locations and working arrangements; and • Health and wellbeing support arrangements are accessible across different staff groups, including wholetime and on-call employees, with any barriers to access identified and addressed.
	The following areas of good practice were identified: • There is a comprehensive suite of guidance available to managers which allows for clear direction on their sickness absence responsibilities. • All health and wellbeing resources are widely available to staff through the Service's CONNECT/Safe2b intranet pages. • Wellbeing resources are actively promoted through multiple communication channels and supported by reviews of communication effectiveness.	

Other Relevant Information

We are aware of current limitations in the reporting functionality within the HR system, iTrent, with attendance management monitoring relying on manual processes. Management has confirmed that a programme of work is underway with the Data Analytics team, overseen by the Senior Leadership Team (SLT), to enhance dashboard and reporting capabilities. As this improvement work is already in progress and subject to oversight, no separate finding or action has been raised within this report.

Audit Findings & Management Action Plan – October 2026

Finding 1 – Health and Wellbeing Resources Annual Review	Action
Historically, the review of wellbeing resources has largely been undertaken on a reactive basis in response to identified issues, changes in services or resource requirements. Whilst the appointment of the Health and Wellbeing Project Officer has introduced arrangements for annual reviews going forward, there is currently no formal framework or checklist in place to ensure reviews are consistently informed by key information such as sickness absence trends, causation data, utilisation reports, outcomes achieved and staff feedback. In addition, although management receives data from wellbeing providers and sickness absence reporting, there is limited evidence of a structured assessment of whether available resources remain targeted towards the primary causes of absence and continue to meet evolving workforce needs. This is also apparent, as it was identified that a health and wellbeing questionnaire is available to all staff via CONNECT. However, only three responses have been received since 2021. Without a formal, data-led review process, the Service may not be able to demonstrate that wellbeing resources remain effective, relevant and aligned to the main causes of sickness absence and workforce need. This could result in resources becoming outdated, gaps in support not being identified promptly, and opportunities to improve employee wellbeing and attendance outcomes being missed.	Implement a formal annual review process for wellbeing resources, supported by a documented checklist. This review should consider: • Analyse sickness absence trends and assess whether current wellbeing provisions contribute to either a reduction in sickness absence and/or the current provisions remain aligned to workforce needs; • Ahead of the annual review, promote completion of the health and wellbeing questionnaire to review any staff feedback (e.g. staff questionnaire results and actions from the Operational Effectiveness Database) and consider whether any updates are required to be actioned across wellbeing provisions; • Review of CONNECT/Safe2b wellbeing pages to ensure all information is still accurate. Following completion of the annual review, any actions requiring updates to wellbeing provisions should be documented and tracked through to their resolution. **Management Response:** Management accepts the action. A documented annual review and checklist will be introduced, drawing on sickness absence trends, service utilisation and outcomes, staff feedback, and a review of CONNECT/Safe2b content. The review will also incorporate any accessibility issues (see Findings 3 & 4). Any resulting improvements will be recorded, assigned and tracked to completion.

Priority	2	**SWAP Reference**	AP #10788
Responsible Officer		Health and Wellbeing Project Officer	
Timescale		31 March 2027	

Finding 2 – Attendance Management Procedure Review	Action
The Attendance Management Procedure was found to be current, subject to an established review cycle, and aligned to the key legislative requirements applicable at the time of its most recent review. However, we identified that more recent employment legislation introduced since the procedure was last reviewed, such as the Employment Rights Act 2025, have been implemented in practice, however, this has not been reflected within the procedure or supporting documentation. The Head of People Support advised that these updates are being considered through the current review underway of the Attendance Management Procedure and supporting guidance. Until the next review is completed, there is a risk that managers may not have visibility of the most up-to-date legislative developments through the attendance management documentation, potentially reducing assurance that guidance remains aligned to current employment law requirements.	Ensure the Attendance Management Procedure and associated guidance are reflective of recently introduced employment legislation. **Management Response:** Management accepts the action. The current review of the Attendance Management Procedure and supporting guidance will incorporate relevant recent employment legislation, with the revised documents subject to the established consultation, approval and communication process.
	Priority 3 — **SWAP Reference** AP #10778
	Responsible Officer Health and Wellbeing Project Officer
	Timescale 30 November 2026

Finding 3 – Review of Accessibility of Wellbeing Services	Action
The Service provides a range of wellbeing resources that are available to all staff groups. However, discussions during the review with the Head of People Support identified that some services, such as physiotherapy provision, are currently delivered through limited appointment availability, which may not always align with the working arrangements of on-call staff who have commitments with primary employers. Whilst no specific accessibility concerns were identified during testing, management recognised that there may be value in periodically reviewing the accessibility of wellbeing services and considering whether alternative referral routes, appointment arrangements or delivery methods would further support access for all staff groups. If wellbeing services are not periodically reviewed from an accessibility perspective, there is a risk that some staff groups may find it more difficult to access available support, potentially reducing uptake and limiting the effectiveness of wellbeing initiatives.	Undertake a review of wellbeing service accessibility for different staff groups, including on-call employees, and consider whether alternative referral routes (e.g. vouchers), appointment availability or methods of service delivery would further improve access to support where appropriate. **Management Response:** Management accepts the action. Accessibility of wellbeing services will be reviewed across staff groups, including on-call employees, and proportionate options for referral routes, appointment availability and alternative delivery methods will be considered and implemented where appropriate. The delivery methods and appointment availability will be considered as part of the wider Occupational health Procurement which will be concluded November 2027.
	Priority 3 — **SWAP Reference** AP #10795
	Responsible Officer Head of People Support
	Timescale 30 November 2027

Finding 4 – Reporting of Wellbeing Access Issues	Action
Health and Wellbeing resources are available to all staff through CONNECT, and the Head of People Support advised that any issues accessing wellbeing support would be raised with them. However, the process for reporting access issues or barriers to support is not formally documented or communicated to staff. As a result, there is limited assurance that all access barriers are consistently identified, reported and resolved. Without a clearly communicated route for reporting access issues, barriers to wellbeing support may not be identified or escalated in a consistent manner. This could limit the Service's ability to understand and respond to accessibility concerns and ensure support arrangements remain effective for all staff groups.	Document and communicate the process for reporting wellbeing resource access issues and barriers to support. Consider including this within CONNECT wellbeing pages and/or new starter wellbeing communications so that staff are aware of how issues can be raised. **Management Response:** Management accepts the action. A clear route for reporting and escalating wellbeing access issues will be documented and communicated through the CONNECT wellbeing pages and relevant staff communications, with reported barriers recorded and followed through to resolution. This will also be reported within each annual review.
	Priority 3 — **SWAP Reference** AP #10794
	Responsible Officer Health and Wellbeing Project Officer
	Timescale 31 March 2027

Appendix 1 – 2026/27 Audit Plan and Performance

Audit Name	Healthy Organisation Theme	Linked To	Status	Opinion	No of Actions	Actions		
						1	2	3
Malpractice Management – Complaints	Corporate Governance	Strategic Risk 598 HMICFRS People Pillar Priority 5	Final	Substantial	3	-	1	2
Business Continuity	Corporate Governance Risk Management	HMICFRS Efficiency Pillar Priority 4	Final	Substantial	2	-	1	1
Accounts Payable	Financial Management	Strategic Risk 0006 HMICFRS Efficiency Pillar Priority 4	Final	Reasonable	4	1	2	1
Accounts Receivable	Financial Management	Strategic Risk 0006 HMICFRS Efficiency Pillar Priority 4	Final	Reasonable	3	-	3	-
Cyber Security	Information Management	Strategic Risk 301 HMICFRS Efficiency Pillar Priority 4	Final	Reasonable	9	-	7	2
Health and Wellbeing Arrangements	People and Asset Management	Strategic Risk 598 HMICFRS People Pillar Priority 5	Final	Reasonable	4	-	1	3
Energy Management & Environmental Considerations	People and Asset Management	HMICFRS Efficiency Pillar Priority 4	Planning	-	-	-	-	-
Skills Management and Competency Recording	People and Asset Management	HMICFRS People Pillar Priority 5	Planning	-	-	-	-	-
Follow Ups	All	All	-					

Internal Audit Plan Progress 2026/27 Quarter 3

The performance results for progress against the internal audit plan for Quarter 3 of the 2026/27 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 on target.