SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 3.1

Meeting	**Audit, Risk and Assurance Committee**
Date	**9 May 2024**
Location	**Via Video Conference**
Title of Paper	**Internal Audit Reports**
Presented By	**John McNellis** **Head of Finance, Audit and Risk** **Claire Robertson, BDO**
Recommendation to Members	**For discussion**
Appendix Attached	**Yes –** **Appendix A – Grievance Process** **Appendix B – IT General Controls** **Appendix C - Best Value Readiness**

PURPOSE

To present the Audit, Risk and Assurance Committee (ARAC) with the internal audit reports on the Grievance Process, IT General Controls and Best Value Readiness from the 2023/24 internal audit plan.

The paper is presented in line with the corporate governance framework of the Scottish Police Authority (SPA) and Audit, Risk and Assurance Committee (ARAC) terms of reference and is submitted for consultation.

1 BACKGROUND

1.1. The Internal Audit plan for 2023/24 was approved by the ARAC in January 2023.

1.2. The following audits have been completed as part of the Internal Audit Plan:

- Grievance Process
- IT General Controls
- Best Value Readiness

2 FURTHER DETAIL

Grievance Process (Appendix A)

a. Background:

- This review covers the design and operation of controls relating to the grievance process in place, to provide assurance over the design and operational effectiveness of the grievance processes.

b. Internal Audit Findings:

- **Limited assurance** has been provided over the design and operational effectiveness.
- BDO can see that clear steps are being taken to improve the culture within the organisation and further develop softer skills. This is being done through the creating a positive workplace programme, which includes actions being taken to roll out people manager training, further mediation support, and raising awareness on the support and services in place. However, a number of important findings were raised.
- Key themes of the findings include:
  - ➢ Introducing enhanced grievance governance and performance reporting, in particular to the SPA Board or Committee level.
  - ➢ Grievance processes and supporting documentation being completed in full compliance with the grievance process procedure in place.
  - ➢ Introducing ongoing grievance process feedback mechanisms.
- Actions to address previously identified grievance process recommendations are ongoing, and that the impact of rolling out the creating a positive workplace programme on culture and confidence in the grievance process cannot yet be assessed.

c. Summary of Findings of the Report:

SUMMARY OF FINDINGS		# OF AGREED ACTIONS
High	2	3
Medium	2	3
Low	1	3 (2 actions were not accepted by the management)
TOTAL NUMBER OF FINDINGS: 3		9

d. SPA Considerations:

- There has been significant focus on values and standards, what they mean and what is expected from those who represent the police service. All within the police service have a duty to challenge and report unacceptable behaviours and improper conduct when they encounter it.
- SPA welcomes the internal audit report findings. We note that all high and medium related actions have been agreed with short implementation dates set.
- Two low risk actions have not been agreed to. We recognise that management has provide rational for this decision.

IT General Controls (Appendix B)

a. Background:

- This report contains the findings from the IT General Controls (ITGC) review as part of the 2023-24 internal audit plan.
- The following areas were covered as part of the scope of this report:
  - IT Strategy and Governance
  - Physical Security of server environment(s)
  - User access, including user provisioning, leavers, privileged access management and password configuration standards
  - IT hardware and software asset management
  - Vulnerability management
  - IT change management
  - IT infrastructure performance and capacity management
  - Incident and problem management
  - Back-up and recovery procedures
  - Third Party Management.

b. Internal Audit Findings:

- **Moderate assurance** is provided on the design of IT general controls based on our assessment covering ten domains
- The 'Medium' significance findings are related to:
  - A lack of periodic user access reviews;
  - Password policies for legacy systems require an assessment; and
  - Limitations impacting patch management.

c. Internal Summary of Findings of the Report

SUMMARY OF FINDINGS		# OF AGREED ACTIONS
High	0	0
Medium	3	7
Low	3	6
TOTAL NUMBER OF FINDINGS: 6		13

d. SPA Considerations:

- SPA welcomes the findings of the audit which concludes there are 'generally sound' controls with some exceptions.

- All findings have been accepted and we note that in some cases the completion deadline is long which can be partly related to the time require to implement IT related changes.
- The 2024-25 internal audit plan includes a place holder for a further IT related audit. The findings of the general controls audit will be considered when scoping the next IT audit.

Best Value Readiness (Appendix C)

a. Background:

- The purpose of this review is to provide advice on Police Scotland’s Best Value assessment readiness.
- This advisory review was carried out by BDO by informed discussions with key members of staff. They reviewed key documentation to understand and assess the work undertaken in establishing a Best Value approach and plans going forward on how they will deliver their outcomes.

b. Internal Audit Findings:

- The review has highlighted some observations that present risk to the Best Value approach:
  - ➢ Resourcing constraints: There is no clear pathway on how resource requirements will be fulfilled, including feasibility of using additional/external staff to be able to achieve operational delivery of Best Value.
  - ➢ Project progress: There has been no oversight and sign-off on the current status of the project as progress reporting has been paused.

c. Internal Summary of Findings of the Report

SUMMARY OF FINDINGS		# OF AGREED ACTIONS
High	1	2
Medium	1	2
Low	4	5
TOTAL NUMBER OF FINDINGS: 6		9

d. SPA Considerations:

- SPA welcomes the work being undertaken by Police Scotland to address their Best Value responsibilities.
- The internal audit report provides assurance on progress and moving forward addressing the recommendations.
- ARAC will continue to monitor progress of the Police Scotland best value journey including the findings from this audit.

3 FINANCIAL IMPLICATIONS

3.1 There are no specific financial implications from this report, however, the implementation of some actions is likely to require financial resources.

4 PERSONNEL IMPLICATIONS

4.1 There are personal implications highlighted in the grievance process internal audit report.

5 LEGAL IMPLICATIONS

5.1 There are no specific legal implications associated with this paper. Reviews will consider applicable legal implications.

6 REPUTATIONAL IMPLICATIONS

6.1 All of these reports may have reputational implications if the service is unable to address the issues raised or there are reputational consequences from the findings.

7 SOCIAL IMPLICATIONS

7.1. There are no social implications in this report.

8 COMMUNITY IMPACT

8.1 There are no community implications in this report.

9 EQUALITIES IMPLICATIONS

9.1. There are no equalities implications in this report.

10 ENVIRONMENT IMPLICATIONS

10.1. There are no environmental implications in this report.

RECOMMENDATIONS

Members are invited to discuss and note the internal audit reports. All recommendations will be subject to regular follow up reporting to this committee.

SCOTTISH POLICE AUTHORITY & POLICE SCOTLAND

GRIEVANCE PROCESS - FINAL

APRIL 2024

LEVEL OF ASSURANCE:	
DESIGN	LIMITED
EFFECTIVENESS	LIMITED

IDEAS | PEOPLE | TRUST

CONTENTS

DISTRIBUTION LIST		
FOR ACTION	DARREN PATTERSON	HEAD OF WORKFORCE GOVERNANCE
	NICKY PAGE	DEPUTY DIRECTOR OF PEOPLE AND DEVELOPMENT
FOR INFORMATION	AUDIT, RISK & ASSURANCE COMMITTEE	MEMBERS

REPORT STATUS	
LEAD AUDITOR(S):	JOE REID & SEAN MORRISON
DATES WORK PERFORMED:	11 DECEMBER 2023 - 02 APRIL 2024
DRAFT REPORT ISSUED:	09 APRIL 2024
MANAGEMENT RESPONSES RECEIVED:	30 APRIL 2024
FINAL REPORT ISSUED:	30 APRIL 2024

RESTRICTIONS OF USE

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)		
DESIGN	Limited	System of internal controls is weakened with system objectives at risk of not being achieved.
EFFECTIVENESS	Limited	Non-compliance with key procedures and controls places the system objectives at risk.

SUMMARY OF FINDINGS (SEE APPENDIX I)		
H	2	🟥
M	2	🟧
L	1	🟩
TOTAL NUMBER OF FINDINGS: 5		

BACKGROUND

It was agreed with management and the Audit, Risk and Assurance Committee as part of the 2023-24 internal audit plan that Internal Audit would undertake a review of the grievance process.

The grievance process is an important method of ensuring staff wellbeing and engagement. When staff have a problem or concern the grievance procedure should be used to try and resolve any issues in the workplace.

Examples of grievances can include:

- Terms and conditions of employment
- Health and safety
- Bullying and harassment
- Discrimination
- Working environment

It is encouraged that problems or concerns are dealt with at the time or through a line manager, however if the problem is not resolved, or deemed ‘more significant’, a formal grievance procedure is in place to support and guide staff on the actions to be taken. The grievance procedure outlines the steps that are taken in the grievance process, including timescales for completion, meetings undertaken, outcomes and the appeals steps. Roles and responsibilities are also outlined for staff, management, witnesses, subjects and the Executive team.

The procedure is being refreshed and at the time of the audit was in consultation, the updated procedure aims to enhance the steps that can be taken to resolve an issue prior to it becoming a formal grievance.

To support the effective utilisation of the grievance process, a number of toolkits have been produced. Also, to enhance the internal knowledge, training has been provided on mediation and all supervisors are required to undertake the newly rolled out people management development programme, which covers grievances and development of associated behavioural skills, aimed to be completed by the end of 2024.

A case compliance panel is in place for Police Scotland staff and officers, and part of their remit is to review grievance cases to ensure that the process has been followed, to identify trends in the issues, and put in place actions to address any lessons learnt.

Professionalism Management Board (PMB) is also in place for Police Scotland officers, which receives information on all new grievances raised and is provided with periodic updates on the significant cases and annual trend information. All cases are tracked through to closure.

The Case Allocation Review Panel (CARP) reviews each grievance and assesses the legal implications of the grievance raised, the procedure to be followed, suggests options to enable a successful solution, and has attendance of HR, Legal and Professional Standards. Meeting notes are maintained for each grievance case.

Grievances are tracked via a number of methods including an excel tracker which details employment type, PSI number, name, overview of grievance, reason for delay, CARP guidance, priority status, appeal information, investigating manager, organisational learning and key timescales for live and archives cases.

Documentation is also maintained within a secure SharePoint, which has information on case details, key dates, appeals, resolved date, case status and can be used to store confidential case documents. Case documents are primarily stored within the secure network drive.

To improve the awareness of the grievance process, and managing workplace issues the creating a positive workplace (CAPW) programme was commenced in 2023, initiated as a result of internal reviews, the raising an issue and grievance survey and external reviews. The programme includes communications initiatives, line manager briefings, notifications on the intranet, and training to people managers and training mediators. The campaign places an importance on mediation, culture and softer skills within the workplace.

EXECUTIVE SUMMARY

BACKGROUND (continued)

In 2022 the Research and Insight team conducted a survey around raising an issue and grievance within the SPA and Police Scotland. The survey was communicated via the intranet, and it was explained that the findings from the survey were to be used to inform consideration of policy, process, training, and the culture of the organisation. The survey targeted anyone who had raised a grievance or issue, had a grievance raised against them, line managers involved, grievance investigating officers, witnesses, staff accompanying colleagues and HR practitioners. The survey opened on 20th September 2022 and closed on 2nd November 2022.

Following the closure of the survey, the Research and Insight Team processed the results and in January 2023 reported on the work they completed on behalf of People & Development to understand the colleague experience of raising an issue and a grievance. Actions identified from the survey included required culture changes, awareness raising of support available, training for management and supervisors, triaging and filtering early in the grievance process, investigating officer availability and dedicated time to the grievance, and external support.

The results of the survey were distributed to Line Managers via a corporate communications email and communicated on the organisation intranet, which provided the results of the survey and what next steps had been identified. The results were also presented to the Director of People and Development, then the Executive Team.

Performance/progress reports on actions taken in relation to the survey actions and creating a positive workplace were presented to a range of recipients including, People & Development, SLB, Policing Together SOB, SMT, and Trade Union.

SCOPE

This review covers the design and operation of controls relating to the grievance process in place. The risks scoped within the review are detailed in Appendix III which is an extract from the agreed terms of reference.

PURPOSE

The purpose of this review was to provide management and the Audit, Risk and Assurance Committee, with assurance over the design and operational effectiveness of the grievance processes in place within Police Scotland and the Scottish Police Authority.

CONCLUSION

We can provide limited assurance over the design and operational effectiveness of the organisation's grievance processes. We can see that clear steps are being taken to improve the culture within the organisation and further develop softer skills through the creating a positive workplace programme, which includes actions being taken to roll out people manager training, further mediation support, and raising awareness on the support and services in place.

However, five findings have been raised, with two rated as high, two as medium and one as low. Key themes include:

- Introducing enhanced grievance governance and performance reporting, to the SPA Board or sub-Committee level.
- Grievance processes and supporting documentation being completed in full compliance with the Grievance procedure in place.
- Introducing ongoing grievance process feedback mechanisms.

Internal Audit note that actions to address previously identified grievance process recommendations are ongoing, and that the impact of rolling out the creating a positive workplace programme on culture and confidence in the grievance process cannot yet be assessed.

OUR TESTING DID NOT IDENTIFY ANY CONCERNS SURROUNDING THE CONTROLS IN PLACE TO MITIGATE THE FOLLOWING RISK:

✓ Personnel may have inappropriate access to the data within the grievance tracker and People Direct due to the organisations not having appropriate technical controls in place to manage, remove and review user access to the system and modules.

FOR THE FOLLOWING RISKS, WE HAVE RAISED NO FURTHER FINDINGS BUT NOTE THAT RECENT FINDINGS ARE STILL BEING ACTIONED AND THE IMPACT OF ONGOING INITIATIVES HAS NOT YET BEEN ASSESSED IN THESE AREAS:

✓ Staff are unable to or do not have the confidence to raise a grievance due to there being a negative culture or lack of confidential processes for raising a grievance.

✓ Previously identified grievance process failings are not addressed, or actions suitably tracked resulting in reputational failings and legal damage being incurred.

EXECUTIVE SUMMARY

SUMMARY OF GOOD PRACTICE

During our review, we identified a number of areas of good practice:

- The grievance procedure outlines detailed information on the steps to be taken to raise and handle a grievance and appeals process, and includes detailed roles and responsibilities, timescales, meetings, as well as supporting guides and FAQs.
- The organisation have commenced the creating a positive workplace programme which aims to improve the culture within the organisation and as part of this have begun rolling out the people manager development programme, to enhance manager soft skills. The programme has incorporated learnings and actions from both external and internal reviews on culture and grievances.
- An extensive survey was undertaken in 2022 and early 2023 which gathered information on staff experiences and perceptions of the grievance process. Following completion of the survey, the results were reported to management and staff, and progress updates were reported to groups such as the senior management team and the trade unions at the end of 2023.
- Grievance information is maintained in secure environments to ensure that staff do not have inappropriate access to confidential information.
- The Case Compliance Panel and Case Allocation Review Panel are in place to review grievance cases.

SUMMARY OF FINDINGS

Notwithstanding the area of good practice identified, we identified the following opportunities for improvement, which are summarised below:

- **Grievance Governance Reporting -** There is currently no reporting on grievances, and it was noted by management that the last report on grievance performance to the SPA was in 2020. Therefore, there is no reporting on early and effective resolution, grievances upheld, statistics or KPIs, themes and trends, lessons learnt, or actions being taken to improve timescales around grievance completion.
- **Grievance Process Compliance** - Internal Audit selected a sample of fifteen grievance cases split between live and archived within 2023 to test the extent to which procedures were followed consistently, in good time, and to assess record keeping. A number of points have been noted on slide 8, and in particular, the key themes related to gaps in record keeping evidencing the grievance procedure steps and procedure timescales within the process not being achieved.
- **Grievance Tracking -** Internal Audit note that there are multiple methods used to track grievance cases and maintain supporting evidence and timescales recording, for example using the grievance tracker spreadsheet, the people direct portal and a secure SharePoint. Internal Audit reviewed the grievance tracker and upon review identified that there is missing information within the tracker for both live and archived grievances. For example, there are gaps in key dates, investigating officer, learnings, CARP and Case Compliance Panel dates and guidance, and appeal information.
- **Feedback and Lessons Learnt -** There are no formal requirements or channels in place for feedback to be provided on completed grievances to identify potential improvements or lessons to be learnt on what is working well, in particular for investigating officers.
- **Grievance Documented Policies and Procedures -** Internal Audit note that the grievance procedure has clear guidance on the steps to be followed when initiating a grievance, managing a grievance, timescales and appeals. However, the following points have been noted:
  - It is unclear in the previous and proposed grievance procedure what success criteria, aims and objectives are in relation to a grievance.
  - There is also an opportunity to clearly record the required approvals for publishing the process document, including whether the SPA Board is required to provide oversight and approval.
  - The Grievance process outlines that there is a requirement for evidence relating to grievances to be maintained within the People Direct Portal. However, upon discussion with management it has been outlined that the People Direct Portal is not suitable for storing confidential grievance supporting documentation and that the system is not used for maintaining grievance case evidence.

  Supporting guides and toolkits will be required to be updated to reflect any material changes between the current and proposed grievance process once approved and implemented.

DETAILED FINDINGS

DETAILED FINDINGS

RISK: INAPPROPRIATE ACTIONS ARE TAKEN BY THE BOARD AND MANAGEMENT IN RELATION TO GRIEVANCE MATTERS DUE TO THERE NOT BEING A CLEAR GOVERNANCE STRUCTURE IN PLACE FOR DELIVERING AND REPORTING ON GRIEVANCES THROUGHOUT POLICE SCOTLAND AND THE SCOTTISH POLICE AUTHORITY.

FINDING 1 - GRIEVANCE GOVERNANCE REPORTING			TYPE
The oversight of both the SPA and Police Scotland should be sufficient to scrutinize the effectiveness of the grievance process, and to ensure that lessons are being learnt and actions taken on grievance themes and performance issues in relation to procedure compliance. It was noted by management that the last report on grievance performance to the SPA was in 2020. Therefore, there is no reporting on early and effective resolution, grievances upheld, statistics or KPIs, themes and trends, lessons learnt, or actions being taken to improve timescales of grievance completion. Management stated that the current HR infrastructure both in terms of system capabilities and resource have made it difficult for grievance reporting to be completed.			DESIGN
IMPLICATION			SIGNIFICANCE
From a governance perspective the SPA Board or relevant sub-committees are not being provided with sufficient information to assess how the organisation is performing in relation to grievances and as a result are unable to make appropriate decisions and have a lack of oversight in relation to grievance matters.			HIGH
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that steps are taken to introduce regular grievance performance reports, including the following information: • Grievance statistics, such as ongoing, completed, appeals • Grievance timescales and a RAG rating showing compliance with the documented process timescales • Grievances upheld or dismissed • Grievance themes and trends • Lessons learnt on completed grievances • Actions taken to improve grievance compliance with the documented process As noted in the findings throughout the report an HR system would make the process for developing reports efficient and reduce the risk of manual human errors and as a result increase the reliability of reporting in alignment with good practice.	Head of Human Resources	Management accepts the recommendation. We agree we should report on grievances with regular frequency and in particular lessons to learn. This is somewhat hampered by current structures and a lack of IT infrastructure to support the efficiency of reporting. We will commit to providing iterative grievance performance reports based on current staffing and structures but this will be limited until such a time that investment is made in an HR system.	December 2024

DETAILED FINDINGS

RISK: INAPPROPRIATE ACTIONS ARE TAKEN BY STAFF WHEN USING EITHER THE GRIEVANCE TRACKER OR PEOPLE DIRECT FOR RECORDING GRIEVANCES DUE TO THERE BEING A LACK OF A CONSISTENT APPROACH FOR RECORDING AND STORING GRIEVANCE PROCESS INFORMATION.

FINDING 2 - GRIEVANCE PROCESS COMPLIANCE	TYPE
The grievance procedure should be followed in a consistent and timely manner. This will help to ensure that the process is conducted effectively and efficiently. Records of all actions and correspondence should be maintained to evidence that all duties have been discharged as required by the procedure to prevent any future action being taken against the organisation. We selected a sample of fifteen grievance cases split between live and archived within 2023 to test the extent to which procedures were followed consistently, in good time, and to assess record keeping. The following exceptions were identified: • Three instances where evidence of the grievance being received could not be provided • Four instances where the initial grievance letter did not include the desired outcome from the grievance • Seven instances where the Grievance was not forwarded onto the People Direct Online Portal • Ten instances where the time taken to appoint an investigating manager was not satisfactory or there was no record of date of appointment within the tracker • Two instances where there was no evidence suggesting informal resolution was attempted. • Eleven instances where the grievance meeting was not held within 14 days of receiving the grievance. • One instance where no invite letter could be evidenced for the grievance meeting • Ten instances where the notes document from the grievances meeting was not signed by all in attendance • One instance where the correct note taking template was not used for the grievances meeting • Four instances where no evidence was available to verify whether notes were shared following the grievances meeting • Three instances where the outcome letter was not provided within 7 calendar days of the grievance concluding • Four instances where it was unclear when the grievance was concluded so timeliness of the outcome letter could not be assessed • Fourteen instances where all evidence was not uploaded to the People Direct Online Portal Of the samples where an appeal was raised (eight) the following issues were identified – Internal Audit note that per the tracker four of these were ongoing: • Three instances where the appeal was not submitted within 7 days of the outcome letter • Six instances where the appeal meeting was not held within 14 calendar days of the appeal being submitted • Four instances where the invite letter to the appeal meeting could not be evidenced • One instance where notes from the appeal meeting could not be evidenced • One instance where there was no evidence to support notes from the appeal meeting being circulated	EFFECTIVENESS

DETAILED FINDINGS

RISK: BUDGET PRIORITISATION IMPACTS ARE NOT FULLY CONSIDERED RESULTING IN A NEGATIVE IMPACT ON STAFF WELLBEING, QUALITY OF POLICING AND ESTATES DETERIORATION.

IMPLICATION			SIGNIFICANCE
There is a risk that the organisation does not achieve the intended outcomes of the grievance process if it cannot sufficiently evidence that the prescribed procedures were followed consistently and in a timely manner, where records including key documents and correspondence are not suitably maintained this can result in an increased risk of reputational or legal action being successful against the organisation in cases where further action is taken by those involved in a grievance.			HIGH
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
It has been consistently identified within the HR related audits undertaken that investment in an effective HR system would allow the organisation to enhance the capabilities in place to consistently and efficiently manage and report on HR matters and reduce the risk of manual errors and lost records. The following recommendation was raised within the Ill Health Retirements and Injury audit report which would also be applicable and improve the capabilities in place to manage grievances: *"Management should evaluate the feasibility of introducing a formal case management system to record, manage, and monitor all individual IHR and IoD applications. Consideration should be given to a system which can provide more automation around tracking case progress and timescales and can flag to staff where a case has not progressed or has been stagnant for a period of time (e.g. by setting a pre-determined criteria). A suitable case management system should also allow effective record keeping by acting as a repository for all key documentation, correspondence, and case notes to be stored securely within individual case files."*	Head of Human Resources	Management accepts the recommendation. We will pursue the options available for an HR System that meets the needs of the organisation across a number of HR disciplines. In the absence of this system we have recorded a risk.	September 2024
Until a new system has been implemented, we recommend that spot checks are conducted over a sample of completed grievances on a regular (e.g., quarterly) basis to verify that the documented grievance procedure has been followed and all relevant documentation sufficiently retained. Where gaps are noted, these should be rectified within a suitable timeframe and lessons learnt conducted on repeated cases of non-compliance with the procedure requirements.	Head of Human Resources	Management accepts this recommendation. Based on the resource available we will consider introducing spot checks as recommended.	September 2024

DETAILED FINDINGS

RISK: INAPPROPRIATE ACTIONS ARE TAKEN BY STAFF WHEN USING EITHER THE GRIEVANCE TRACKER OR PEOPLE DIRECT FOR RECORDING GRIEVANCES DUE TO THERE BEING A LACK OF A CONSISTENT APPROACH FOR RECORDING AND STORING GRIEVANCE PROCESS INFORMATION.

<table>
<tr><th colspan="3">FINDING 3 - GRIEVANCE TRACKING</th><th>TYPE</th></tr>
<tr><td colspan="3">It is essential that grievance cases are tracked in a consistent manager and information is overseen to ensure that grievances are completed in line with the documented procedure in place. Effective tracking also provides management with accurate information to identify potential cases with issues or delays.
Internal Audit note that there are multiple methods used to track grievance cases and maintain supporting evidence and timescales recording, for example using the grievance tracker spreadsheet, the people direct portal and a secure SharePoint.
Internal Audit reviewed the grievance tracker and upon review identified that there is missing information within the tracker for both live and archived grievances. For example, there are gaps in key dates, investigating officer, learnings, CARP and Case Compliance Panel dates and guidance, and appeal information.</td><td>DESIGN & EFFECTIVENESS</td></tr>
<tr><th colspan="3">IMPLICATION</th><th>SIGNIFICANCE</th></tr>
<tr><td colspan="3">There is a risk that grievances are ineffectively tracked and overseen to ensure that all required steps have been completed, evidence maintained, and timescales met and recorded. To align with good practice there is an opportunity to reconcile the different methods used to track grievance cases.</td><td>MEDIUM</td></tr>
<tr><th>RECOMMENDATIONS</th><th>ACTION OWNER</th><th>MANAGEMENT RESPONSE</th><th>COMPLETION DATE</th></tr>
<tr><td>We recommend that steps are taken to fully complete and maintain the grievance tracker in place which could be used as a basis for developing management information as noted in recommendation 1 and used as an up-to-date source for management oversight of cases, case learnings, timescale issues and process compliance.
A modern HR system would mitigate the requirement for using SharePoint and spreadsheet trackers.</td><td>Head of Human Resources</td><td>Management accept the recommendation. We will remind staff of the importance of completing all fields within the tracker and will use the periodic reconciliations carried out below as a way of reinforcing this.</td><td>September 2024</td></tr>
<tr><td>Periodic reconciliations should be conducted between the tracker, People Direct Portal and the SharePoint used to track grievances to ensure that there are no discrepancies between the different methods used to track grievance cases, supporting documents and their status.
A modern HR system would provide a single source of data and supersede this recommendation once implemented.</td><td>Head of Human Resources</td><td>Management accept the recommendation. We will commit to undertaking periodic reviews of data as per the recommendation in line with the resource available.</td><td>September 2024</td></tr>
</table>

DETAILED FINDINGS

RISK: THERE ARE CONSISTENT FAILINGS IN THE GRIEVANCE PROCESS WHICH ARE NOT IDENTIFIED AND ACTED ON DUE TO A LACK OF BOTH TREND ANALYSIS AND REMEDIATION ACTION TAKEN BY MANAGEMENT.

FINDING 4 - FEEDBACK AND LESSONS LEARNT	TYPE
Formal feedback channels should be in place to understand the experiences of all individuals involved in a grievance, including Investigation Officers, so that improvements can be identified and implemented for future cases. There are no formal requirements or channels in place for feedback to be provided on completed grievances to identify potential improvements or lessons to be learnt on what is working well, in particular for investigating officers. Support is something that management know is required to be improved based on the 2022 grievance survey results which noted for example that 56% of those who had a grievance against them felt ‘not at all supported’, and as part of the creating a positive workplace programme steps are being taken to enhance the support on offer, raise awareness of support and materials available and to provide more training for those involved in people managing and mediation.	DESIGN & EFFECTIVENESS
IMPLICATION	SIGNIFICANCE
There is a risk that opportunities for improvements within the grievance process are not identified in good time.	MEDIUM

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that a process is put in place to request feedback on completed grievances for those involved, in particular from Investigating Officers, to identify lessons on the grievance process and track whether planned improvements are effective. This could be achieved by introducing a formal debrief process for completed grievances.	Head of Human Resources	Management accept this recommendation. We will consider all options in relation to collating feedback from stakeholders on the grievance process and build this information in to our reporting.	December 2024

DETAILED FINDINGS

RISK: INAPPROPRIATE ACTIONS MAY BE TAKEN BY STAFF IN HANDLING GRIEVANCE PROCEDURES DUE TO LACK OF ROBUST GRIEVANCE POLICIES AND PROCEDURES, AND ROLES AND RESPONSIBILITIES, RESULTING IN REGULATORY ACTION OR REPUTATION DAMAGE TO THE ORGANISATION.

FINDING 5 - GRIEVANCE DOCUMENTED POLICIES AND PROCEDURES	TYPE
Policies and procedures provide staff with guidance on how to discharge their roles and responsibilities and are required to ensure consistency and mitigate the risk of knowledge being lost when staff leave an organisation. The organisation has a Grievance procedure in place, with an updated version in the consultation process at the time of the internal audit, and a range of supporting guides and toolkits in place to provide staff with guidance on the procedures to be followed. Internal Audit note that the procedure has clear guidance on the steps to be followed when initiating a grievance, managing a grievance, timescales and appeals. However, the following points have been noted: • The aims, objectives and resulting success criteria in the previous and proposed grievance procedure are unclear, creating difficulty in being able to routinely monitor its fitness for purpose and that it is being implemented fairly and consistently. As a result, there is a risk of not being able to respond in a timely manner in making necessary improvements to the procedure itself, or to communication and training to support its implementation. • There is also an opportunity to clearly record the required approvals for publishing the process document, including whether the SPA Board is required to provide oversight and approval. Due to the reputational and financial risk that grievance cases can pose to the organisation it is essential that the SPA Board have oversight, confidence and awareness of the grievance process in place, and effectiveness of that process, to discharge their role. • The Grievance process outlines that there is a requirement for evidence relating to grievances to be maintained within the People Direct Portal. However, upon discussion with management it has been outlined that the People Direct Portal is not suitable for storing confidential grievance supporting documentation and that the system is not used for maintaining grievance case evidence. Supporting guides and toolkits will be required to be updated to reflect any material changes between the current and proposed grievance process once approved and implemented.	DESIGN
IMPLICATION	SIGNIFICANCE
There is a risk that the grievance procedure and supporting documents contains inaccurate information, in particular relating to people direct usage.	LOW

DETAILED FINDINGS

RISK: INAPPROPRIATE ACTIONS MAY BE TAKEN BY STAFF IN HANDLING GRIEVANCE PROCEDURES DUE TO LACK OF ROBUST GRIEVANCE POLICIES AND PROCEDURES, AND ROLES AND RESPONSIBILITIES, RESULTING IN REGULATORY ACTION OR REPUTATION DAMAGE TO THE ORGANISATION.

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that management, in line with good practice and its recent commitment in respect of policies more generally, include a section within the grievance procedure outlining its aims and objectives and success criteria, to enable monitoring of fitness for purpose in design and implementation and inform prompt action where issues are identified.	Head of Human Resources	Management do not accept this recommendation. The aims and objectives of the procedure are set out within the procedure, however, not as explicit as ‘aims’ and ‘objectives’. Section 1.1: What is this about? (Aims) This procedure is aimed at resolving workplace issues in a fair and respectful manner, as promptly as possible to prevent escalation and to eliminate discrimination. Section 1.3: Key points (Objectives) We will: do everything we can to resolve it as soon as possible; offer mediation from the outset and at all stages of the procedure; etc. This currently mirrors the other P&D procedures template. Our procedures are developed to ensure clear language is used and our simplified approach means we only provide colleagues with easy to find and relevant information. We do not include all organisational responsibilities such as reporting to SPA within our procedures. As part of our improved performance reporting, we will consider success criteria. However, we will not document this within the procedures. This simplified approach has received positive feedback from the workforce.	N/A

DETAILED FINDINGS

RISK: INAPPROPRIATE ACTIONS MAY BE TAKEN BY STAFF IN HANDLING GRIEVANCE PROCEDURES DUE TO LACK OF ROBUST GRIEVANCE POLICIES AND PROCEDURES, AND ROLES AND RESPONSIBILITIES, RESULTING IN REGULATORY ACTION OR REPUTATION DAMAGE TO THE ORGANISATION.

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that the grievance procedure review and approval process is documented, and that consideration is provided to include SPA Board or sub-Committee approval or oversight within the process.	Head of Human Resources	Management do not accept this recommendation. P&D was given permission to manage its own record set by the Corporate Management Board in 2017. There was no change to the existing governance and approval processes. This was subject to it remaining compliant with the rules set by the Executive and laid out in the Governance of the Police Scotland Record Set. Each year a set number of documents are scheduled for review. This is based on strategy, risk and upcoming legislative change. Departmental priorities are set out in January for the P&D SMT to consider. These are then shared with the JNCC Policies and Procedures subgroup (with updates provided when required). Policies are owned by the Scottish Police Authority and can only be amended through presentation to committee. Early engagement/feedback to SPA may be more suitable with certain procedures to allow for collaborative discussion/transparency.	N/A
We recommend that the grievance process is updated to reflect the required in practice process in relation to utilisation of People Direct Portal, for example if the system is not intended to be used then the procedure should not outline that grievance evidence is maintained within the system.	Head of Human Resources	Management accept this recommendation. The procedure can be updated to reflect the required practice when a defined process for maintaining evidence is defined. Alternatively, wording can be amended to a more generic option: • Details of the grievance and outcomes will be logged with People and Development/People Services. • All documentation must be sent to People and Development/People Services at the end of the procedure.	December 2024

OBSERVATIONS

OBSERVATIONS

- **HR System Capabilities -** Internal Audit previously recommended in the ill health retirements and injury audit that management should evaluate the feasibility of introducing a formal case management system to record and monitor all individual cases. This recommendation also applies to grievances, as a system would enhance the tracking of grievances, improve record keeping and introduce automation opportunities in relation to key steps in the process, including enhancing the performance reporting capabilities. Internal Audit recognise that Management have submitted annual business cases for a HR system in recent years. There will continue to be corporate operational challenges in areas such as human resources if investment is not made to enhance the system capabilities within the organisation.

- **Grievance Training -** Training is essential for ensuring that staff have the required knowledge to discharge their roles and responsibilities in line with the policies and procedures in place within an organisation. The PSNI review on grievance processes within Police Scotland outlined that there were training improvements required, including training required on HR support, mediation, a needs analysis, support toolkits and on grievances. Internal Audit met with a sample of investigating officers, and it was noted that there has been minimal training provided on conducting a grievance investigation. To address these points and other improvement areas identified in the 2022 survey management introduced the people manager development programme in 2023, which aims to train all people managers on areas that would help with handling workplace issues and potentially preventing them resulting in a grievance through early intervention and mediation. The aim is for people managers to have completed this training by the end of 2024. There has also been mediation training provided to personnel to increase the number of mediators within the organisation. Status updates on the training programme progress have been provided to management. Steps are also being taken to enhance the induction process to provide new staff with information on how to raise a workplace issue. Internal Audit note that the training programmes are a work in progress and have not yet been fully rolled out within the organisation.

APPENDICES

APPENDIX I: DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
SUBSTANTIAL	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
MODERATE	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non-compliance with some controls, that may put some of the system objectives at risk.
LIMITED	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
NO	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non-compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
HIGH	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
MEDIUM	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
LOW	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.
ADVISORY	A weakness that does not have a risk impact or consequence but has been raised to highlight areas of inefficiencies or potential best practice improvements.

APPENDIX II: TERMS OF REFERENCE

EXTRACT FROM TERMS OF REFERENCE

PURPOSE

The purpose of this review is to provide management and the Audit, Risk and Assurance Committee with assurance over the design and operational effectiveness of the grievance processes in place within Police Scotland and the Scottish Police Authority.

KEY RISKS

1. Inappropriate actions may be taken by staff in handling grievance procedures due to lack of robust grievance policies and procedures, and roles and responsibilities, resulting in regulatory action or reputation damage to the organisation.
2. Line managers may not have the required knowledge regarding handling a grievance due to there being no training or awareness raising on these topics. Also, staff may not have the awareness on the processes to be followed to raise a grievance.
3. Inappropriate actions are taken by the Board and management in relation to grievance matters due to there not being a clear governance structure in place for delivering and reporting on grievances throughout Police Scotland and the Scottish Police Authority.
4. Inappropriate actions are taken by staff when using either the Grievance Tracker or People Direct for recording grievances due to there being a lack of a consistent approach for recording and storing grievance process information.
5. Issues within the grievance processes are not identified due to there being a lack of oversight controls being in place, for example spot checking of closed grievance cases.
6. Personnel may have inappropriate access to the data within the grievance tracker and People Direct due to the organisations not having appropriate technical controls in place to manage, remove and review user access to the system and modules.
7. Staff are unable to or do not have the confidence to raise a grievance due to there being a negative culture or lack of confidential processes for raising a grievance.
8. There are consistent failings in the grievance process which are not identified and acted on due to a lack of both trend analysis and remediation action taken by management.
9. Previously identified grievance process failings are not addressed, or actions suitably tracked resulting in reputational failings and legal damage being incurred.

APPENDIX III: STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.		
SCOTTISH POLICE AUTHORITY		
DARREN PATTERSON	HEAD OF WORKFORCE GOVERNANCE	AUDIT SPONSOR
POLICE SCOTLAND		
NICKY PAGE	DEPUTY DIRECTOR OF PEOPLE AND DEVELOPMENT	AUDIT SPONSOR
ELIZABETH HOSSACK	REWARD MANAGER	KEY CONTACT
SUSAN BEATON	HEAD OF PEOPLE, HEALTH AND WELLBEING	KEY CONTACT
PAUL STEWART	PEOPLE OPERATIONS MANAGER	KEY CONTACT
MURRAY VALLANCE	SENIOR HR ADVISOR (POLICY)	KEY CONTACT

APPENDIX IV: LIMITATIONS AND RESPONSIBILITIES

MANAGEMENT RESPONSIBILITIES

The Board is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work.

The Board is responsible for ensuring the internal audit function has:

- The support of the Association's management team.
- Direct access and freedom to report to senior management, including the Chair of the Audit Committee.
- The Board is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the Association.

Internal controls covers the whole system of controls, financial and otherwise, established by the Board in order to carry on the business of the Association in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The Board is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Board.

LIMITATIONS

The scope of the review is limited to the areas documented under Appendix II - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of colleagues interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

FOR MORE INFORMATION:

CLAIRE ROBERTSON, HEAD OF DIGITAL & RISK ADVISORY SERVICES - SCOTLAND

+44 (0)7583 237 579
claire.robertson@bdo.co.uk

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

www.bdo.co.uk

Scottish Police Authority

IT General Controls

INTERNAL AUDIT REPORT - FINAL

April 2024

LEVEL OF ASSURANCE:	
DESIGN	MODERATE
EFFECTIVENESS	N/A

IDEAS | PEOPLE | TRUST

CONTENTS

DISTRIBUTION LIST		
FOR ACTION	MARTIN LOW	DIGITAL DIVISION (COO)
	CHRIS PERRY	CHIEF TECHNOLOGY OFFICER
	HAZEL IRVING	HEAD OF ICT SERVICE DELIVERY
	JOE CARRAGHER	HEAD OF APPLICATIONS AND DEVELOPMENT
FOR INFORMATION	AUDIT, RISK & ASSURANCE COMMITTEE	MEMBERS

REPORT STATUS	
LEAD AUDITOR(S):	B DUFFELL-CANHAM & M LEMMER
FIELDWORK PERFORMED:	22 JANUARY 2024 - 15 MARCH 2024
DRAFT REPORT ISSUED:	12 APRIL 2024
MANAGEMENT RESPONSES RECEIVED:	29 APRIL 2024
FINAL REPORT ISSUED	29 APRIL 2024

RESTRICTIONS OF USE

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)		
DESIGN & IMPLEMENTAITON	Moderate	Generally a sound system of internal controls designed to achieve system objectives with some exceptions.
EFFECTIVENESS	N/A	Operational effectiveness has not been assessed as part of this review.

SUMMARY OF FINDINGS (SEE APPENDIX III FOR H/M/L DEFINITIONS)													
H	-												
M	3	🟧	🟧	🟧									
L	3	🟩	🟩	🟩									
TOTAL NUMBER OF FINDINGS: 6													

PURPOSE

The purpose of this review, within the agreed scope, was to provide an assessment of the adequacy of the SPA IT General Control environment based on our testing of the design and implementation of key IT controls.

BACKGROUND

This report contains the findings from the IT General Controls (ITGC) review as part of the 2023-24 internal audit plan.

The Police Scotland ICT Digital division provides IT services to Police Scotland, Forensic Service and SPA Corporate. During the development of the Terms of Reference ("ToR"), we met with key stakeholders to gain an understanding of the Scottish Police Authority's ("SPA") IT landscape. Both the Audit & Assurance and IT teams have recommended a "broad-brush" scope and approach for this audit, with the objective to enable BDO to obtain a more complete understanding of the environment in this initial technology audit , while also identifying areas for deeper examination in future audits.

With this understanding, testing was limited to the design and implementation of the in-scope key controls, with targeted operating effectiveness testing (i.e. sampling operation and effectiveness over a period) being performed in future agreed audits.

The audit team was also requested to incorporate additional IT security control elements to complement the standard ITGC scope. A recent audit had not been taken place on these security topics and the opportunity for independent SME insights on areas for improvement were valued by management.

Overall, the controls selected for review represent a broad set of key "foundational" controls across a broad range of areas, intended to provide SPA with a view of the most significant control issues for management attention.

SCOPE

The following areas were covered as part of the scope of this ITGC review:

1. IT Strategy and Governance
2. Physical Security of server environment(s)
3. User access, including user provisioning, leavers, privileged access management and password configuration standards
4. IT hardware and software asset management
5. Vulnerability management
6. IT change management
7. IT infrastructure performance and capacity management
8. Incident and problem management
9. Back-up and recovery procedures
10. Third Party Management.

APPROACH

Internal Audit conducted walkthroughs with key stakeholders to determine and assess the design of the controls in operation. Evidence was obtained to assess & establish control implementation.

The design of IT controls was assessed against industry standards established in IT control and process frameworks such as COBIT, NIST, ISO and ITIL. The implementation of controls was established by a limited size sample as deemed appropriate for the relevant activity.

Our findings and conclusions formed the basis of the March 2024 exit meeting, where discussions included the factual accuracy of any issues identified. The IA report includes responses from management.

EXECUTIVE SUMMARY

CONCLUSION

Our 'Moderate' assurance conclusion on the design of IT general controls is based on our assessment covering ten domains, where we identified six findings - three assessed as 'Medium' and three as 'Low' significance.

Given the number of areas covered and the relatively low number of significant findings identified, it reflects a good awareness of IT risks and controls by the current management team.

The 'Medium' significance findings are summarised as follows:

Control Design & Implementation

- **A lack of periodic user access reviews:** There is currently no formal process in place to review system privileges on a periodic basis. Management confirmed that informal, ad-hoc reviews do take place.
- **Password policies for legacy systems require an assessment:** We identified numerous legacy systems on SPA servers that do not authenticate using Single Sign-On (SSO) and are not compliant with the password policy requirements as outlined in the Information Security Standard Operating Procedures (SOP).
- **Limitations impacting patch management:** We noted a 53% Microsoft patching non-compliance rate on servers and 82% on other workstations.

We recommend that management prioritise initiatives to address the medium significance findings, especially those relating to user access reviews and patch management.

SUMMARY OF GOOD PRACTICE

We identified several areas of good practice relating to the ITGC Control framework examined, including:

- **IT Strategy:** The development of an IT strategy is a proactive measure that demonstrates a commitment to continuous improvement. SPA approved its IT Strategy in 2023, which includes a 5-year roadmap to support the changing needs of policing.
- **IT Governance Structures:** The establishment of robust governance structures, including monthly IT Board Meetings (focusing on People, Finance and Projects), should facilitate effective oversight and monitoring of IT-related projects, risks, and cybersecurity initiatives.
- **IT Risk Management:** Management has put in place a risk register where risks have been identified with mitigating actions, including review dates when follow-ups are to be conducted.
- **Vulnerability Management:** Regular vulnerability assessments take place, including external penetrations tests.
- **Change Management:** The clear definition and management of different types of changes (CAB, Emergency and Standard) demonstrate a mature approach to change management. The presence of development quality testing and approval processes for normal changes further reinforces the robustness of the change management framework.
- **IT Incident & Problem Management**: Incidents were found to be recorded and managed within the IT Service Management Tool (ITSM), IT Connect. Key performance indicators are measured and reported on a monthly basis.
- **3rd Party Management:** Both on-boarding and Information Security requirements with regards to suppliers has been clearly outlined by the policy.

ACKNOWLEDGEMENT

We would like to thank the management team of the Digital Division for their cooperation and engagement throughout the course of this audit.

EXECUTIVE SUMMARY

KEY FINDINGS

Below is a summary of the key 'Medium' rated findings.

SUMMARISED KEY FINDINGS

REF.	FINDING	TYPE	SIGNIFICANCE
01	**A lack of periodic user access reviews** There is currently no formal process in place to review system privileges on a periodic basis. Management confirmed that informal, ad-hoc reviews do take place. As part of our testing, we cross referenced the HR leavers list for a 12-month period ending 31 December 2023, as well as a list of Active Directory. Furthermore, our analysis of the Active Directory (AD) extraction as of 23 February 2024 revealed discrepancies, including 4 active users with a last logon date exceeding 4 years and 610 active accounts with a last logon date exceeding 90 days. While these issues may not directly compromise security, they pose risks of unauthorised access and indicate insufficient oversight of user accounts.	Design & Implementation	MEDIUM
02	**Password policies for legacy systems require an assessment** Management confirmed that there are legacy systems within SPA servers that do not authenticate using Single Sign-On (SSO) and are not compliant with the password policy requirements as outlined in the Information Security Standard Operating Procedures (SOP). BDO were unable to obtain evidence of password policies for Class 1 systems, where authentication through Active Directory (SSO) is not configured.	Design & Implementation	MEDIUM
03	**Limitations impacting patch management** Our review of the Microsoft System Center Configuration Manager (SCCM) identified the following exceptions: Servers: Non-Compliant - 52.92% Windows Workstation and servers: Non-Compliant - 88.47% Management confirms that patch management is an area of improvement for the Digital Division. Servers were not rebooted after patches were applied due to operational requirements, which likely contributed to the incomplete patches identified. A project has been initiated at the time of our review to remediate these gaps in patch management processes.	Design & Implementation	MEDIUM

DETAILED FINDINGS

DETAILED FINDINGS

RISK: Malicious or accidental changes to sensitive data; inappropriate access to private data

FINDING 1 - A LACK OF PERIODIC USER ACCESS REVIEWS	TYPE
There is currently no formal process in place to review system privileges on a periodic basis. Management stated that informal, ad-hoc reviews do take place. Our analysis of the Active Directory (AD) extraction as of 23 February 2024 revealed discrepancies, including 4 active users with a last logon date exceeding 4 years and 610 active accounts with a last logon date exceeding 90 days. While these issues may not directly compromise security, they pose risks of unauthorised access and indicate insufficient oversight of user accounts.	DESIGN & IMPLEMENTATION
IMPLICATION	**SIGNIFICANCE**
The presence of inactive or outdated accounts may increase the attack surface and exposes SPA to potential security incidents. Moreover, the lack of clear approval details in documentation may result in inconsistent access controls and undermine accountability in user management.	MEDIUM

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
1. A formalised periodic review of user access should be implemented to review the appropriateness of users' access on all systems. Users' access assigned with associated access rights should be assessed by their line manager as part of the review. The review should ensure that system and data access assigned are necessary and commensurate with users' job responsibilities.	1. Richard Allan	1. The CIAM project sets out a new approach to user access management, with the aim being to empower business teams to administer and maintain access to their applications. This will be achieved through the use of an IAM solution, which will automate access where possible and provide mechanisms for direct user requests and periodic reviews through certification campaigns by the business admin users. The CIAM project will perform initial discovery work to identify improvements to: a) Automate the general AD UAM tasks and reviews b) Identify which applications are suitable to migrate to IAM and costs associated with that work. This will then go through a governance process to approve the project scope and required funding.	1. The project is expected to run over several years - end 2026.

DETAILED FINDINGS

RISK: Malicious or accidental changes to sensitive data; inappropriate access to private data

FINDING 1 - A LACK OF PERIODIC USER ACCESS REVIEWS (CONTINUED)			TYPE
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
2. Initiate a thorough review and clean-up of Active Directory accounts, particularly targeting those with last logon dates exceeding specified thresholds. Implement regular monitoring and reporting mechanisms to identify and address inactive or outdated accounts promptly. 3. The process for new starters, Movers, and leavers processes should be documented with version control and approval details. Ensure that the document clearly outlines the information required for user account creation or modification, along with the appropriate approval workflows based on user account types.	2. Craig Worsley 3. David Gillen	2. Management accept this recommendation. Work to complete a review and clean-up of Active Directory accounts is currently underway. This forms part of an overarching Annual Security review that is conducted by our Cyber Security and Assurance team. As part of this review controls will be agreed and regular review periods set up. This review and schedule will be in place by 31st August 2024. We will provide BDO with a view on what controls have been agreed and ensure that the appropriate documentation (including review period) is defined. 3. Digital Division management acknowledges the auditors' findings. There is currently an existing process document for User Account Maintenance which is version controlled with approval details held in SharePoint. A Further review of this document will be complete by the end of May 2024 to ensure that it captures the information noted in this recommendation. Further to this , the document will be updated to reflect the automation provided by the IAM project and will be completed by the end of August 2024.	2. Will have reviewed with schedule in place for user accounts by 31st August 2024 3. Current UAM process to be shared by end of May 2024. Document updates to be captured and process updated by August 2024

DETAILED FINDINGS

RISK: Legacy systems within SPA servers may be exposed to unauthorised access and compromise.

FINDING 2 - PASSWORD POLICIES FOR LEGACY SYSTEMS REQUIRE AN ASSESSMENT	TYPE
Management confirmed that there are legacy systems hosted within SPA servers that do not authenticate using Single Sign-On (SSO) and are not compliant with the password policy requirements as outlined in the Information Security Standard Operating Procedures (SOP). BDO were unable to obtain evidence of password policies for Class 1 systems, where authentication through Active Directory (SSO) is not configured. Management confirmed that when procuring a system, SPA perform a Vulnerability Assessment and Penetration Testing (VAPT) to assess whether the application is secure for use by SPA without the need for SSO. This assessment is part of SPA's assurance process to risk assess and accept the password requirements. Because of the age of the legacy systems used, there is no policy in place for password requirements of these systems.	DESIGN & IMPLEMENTATION
IMPLICATION	**SIGNIFICANCE**
The absence of password policies and SSO authentication on legacy systems increases the risk of unauthorised access to sensitive data, potentially leading to data breaches or compliance violations.	MEDIUM

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
1. Perform an assessment on legacy systems not authenticating through Active Directory to establish the following: • Whether the system password policy is aligned with the Information Security SOP • If not aligned to the SOP, determine whether the SOP password requirements is configurable. 2. Determine the risk and cost/benefit of legacy system developments or upgrades to align the password policy to the SOP requirements.	Joe Carragher	1. Digital Division management acknowledges the findings and will commit to: a) Reviewing the Class 1 systems to assess their compliance with the corporate password policy b) Where not compliant, will establish whether the application's password controls are configurable to make it compliant. 2. Digital Division management acknowledges the auditors' findings and will complete the cost / benefit assessment as recommended.	1. December 2024 2. March 2025

DETAILED FINDINGS

RISK: Systems and servers may be vulnerable to cyber threats.

FINDING 3 - LIMITATIONS IMPACTING PATCH MANAGEMENT	TYPE
With our review of the Microsoft System Center Configuration Manager (SCCM), we identified the following exceptions: Servers: Non-Compliant - 52.92% Windows Workstation and servers: Non-Compliant - 88.47% Management confirms that patch management is an area of improvement for the Digital Division. Servers were not rebooted after patches were applied due to operational requirements, which likely contributed to the incomplete patches identified. A project has been initiated at the time of our review to remediate these gaps in patch management processes.	DESIGN & IMPLEMENTATION
IMPLICATION	**SIGNIFICANCE**
Non-compliance with patching requirements can result in vulnerabilities in systems to known exploits and potentially exposing sensitive data to security threats.	MEDIUM

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
1. Ensure the remediation project aligns its efforts with the patch management improvement initiatives to address identified gaps and proceed with the implementation of necessary changes.	Richard Allan	1. The CTR project is reviewing current patching practices and opportunities to improve. It is expected that there will be several changes to existing patching processes, some of which will be policy and resource driven, whilst others will require changes to technology. These will be implemented in a staged manner, following the appropriate governance and approvals. The Initial Business Case is expected to be approved in June and the Full Business Case along with Procurement activities by December 24. The Strategic Partner will be on-boarded and delivery started February 2025.	1. The CTR work will run until end of years 2025.

DETAILED FINDINGS

RISK: Systems and servers may be vulnerable to cyber threats.

FINDING 3 - LIMITATIONS IMPACTING PATCH MANAGEMENT (CONTINUED)			TYPE
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
2. Management should consider a threat-based assessment to prioritise patching.	Richard Allan	2. Although the management accept this recommendation and the findings noted; this recommendation is in effect already in place. Threat Assessments to prioritise Patching are already completed by the team that supports the Security Operations Centre. Threats are analysed and vulnerability management and patching prioritised according to the risk associated with the threat. As part of the Cyber Threat Reduction (CTR) project and the enhanced Risk Management process being developed by the Cyber Security Service (CSS) project, additional onus and effort will be expended on patching. Senior Management will also have greater visibility into the risks associated with non-compliant patching, which will enable the senior team to determine when activity requires expediated. The new risk management approach will be implemented by the end of December 2024. This will include Power BI reporting providing information on risk and will be presented at Senior Level chaired Groups such as the Outstanding Vulnerabilities Group and the Cyber Strategy Group.	2. The new risk management approach will be implemented by end of 2024.

DETAILED FINDINGS

RISK: Inefficiencies in tracking critical software assets, potentially leading to financial losses.

FINDING 4 - A LACK OF MONITORING UTILISATION OF SOFTWARE LICENCES	TYPE
Although licenses for critical services and applications are subject to monthly reviews and enterprise year-end agreements are in place, there is not a consistent approach to software management to monitor the utilisation of licences by users. The potential risk impact of the finding is considered low due the following mitigations in place: • SPA makes use of SCCM and IT Connect to identify applications installed on devices connected to the network. • End-users are not granted with local admin privileges by default, which prevents the installation of unauthorised applications.	DESIGN
IMPLICATION	SIGNIFICANCE
Without a centralised approach for software asset management, SPA may not be able to efficiently manage the utilisation of software licences, leading to inefficient allocation of resources. Insufficient licences may lead to operational disruption or contractual non-compliance and subsequent penalties by the applicable vendors.	LOW

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
Establish a processes and procedures for regular reviews of licenses and subscription-based services to ensure alignment with business needs and optimise costs, and consider whether a SAM tool would facilitate the software management lifecycle.	Joe Carragher	As noted in the auditors' comments, Digital Division already undertakes regular reviews of application software licensing in relation to business need - this is done as part of annual budget setting and also as part of any software contract renewal or replacement. 1. Management agrees to put in place a policy document that will formalise the need for regular reviews, as detailed above. 2. Digital Division management acknowledges that there is no software asset management tool in place and agrees to progress work on the definition of requirements, costs, etc in relation to the adoption of such a tool.	1. December 2024 2. March 2025

DETAILED FINDINGS

RISK: Inaccuracies in asset reporting, potential loss, misuse of assets, and hinder effective resource allocation

<table>
<tr><th colspan="3">FINDING 5 - INCOMPLETE HARDWARE ASSET REGISTER</th><th>TYPE</th></tr>
<tr><td colspan="3">The asset register maintained by the Digital Division has not been recently been recently reviewed and updated. A number of entries have incomplete fields and client assets do not include sufficient detail such as asset owner and location.
Management stated that auditing of hardware assets is conducted on an ad-hoc basis, rather than through a structured and consistent process.</td><td>DESIGN</td></tr>
<tr><th colspan="3">IMPLICATION</th><th>SIGNIFICANCE</th></tr>
<tr><td colspan="3">Incomplete and inconsistent asset management practices may increase challenges in tracking hardware assets, leading to inefficiencies and poor asset management practises. Additionally, the ad-hoc nature of asset auditing increases the likelihood of oversight and errors in asset management processes, potentially resulting in financial losses and operational disruptions.</td><td>LOW</td></tr>
<tr><th>RECOMMENDATIONS</th><th>ACTION OWNER</th><th>MANAGEMENT RESPONSE</th><th>COMPLETION DATE</th></tr>
<tr><td>1. Management should perform a review of the IT asset register ensuring it accurately reflects the current state of hardware assets. This may involve conducting thorough inventories of key IT assets in all operational locations and storage, and updating records to reconcile with actual assets.
2. Management should investigate the potential root cause and implement measures to address the gap, such as:
• specifically assigning the task of reviewing/auditing asset registers to the appropriate team members
• Introduce mechanisms to support appropriate tracking and monitoring of key IT assets through the full lifecycle.</td><td>Darrell Gough</td><td>A review of the Asset register has been completed and areas of improvement identified with plans in place to address this. These plans will consider identification of appropriate Asset Management and Review process per asset type, as "static" assets (Network switches, Routers, Servers, Storage) are less frequently relocated compared to "end user" assets (Laptops, Desktops, Tablets, etc)
This work will take approximately 1 year to do and is expected to be completed by May 25.
Digital Division will provide detail supporting the actions undertaken to improve the management of the Asset Register.</td><td>May 2025</td></tr>
</table>

DETAILED FINDINGS

RISK: Inadequate oversight of Information Security Standard Operating Procedures (SOP) may lead to inconsistencies and non-compliance.

FINDING 6 - IT POLICIES AND PROCEDURES NOT IN PLACE FOR TWO PROCESSES	TYPE
Although IT policies and procedures are reviewed annually by the Digital Division, the Information Security Standard Operating Procedure (SOP) obtained had not been reviewed since 2021. This SOP is owned by the Information Management team and therefore operates outside of the Digital Division's policy review cycle. A formal policy or procedure document is not in place over the following processes: • Capacity Monitoring: Although alerting is configured for systems to send automatic notifications, a structured framework to guide capacity planning and management activities is not in place • User Access provisioning and deprovisioning: There is no dedicated User Access Management policy or procedure document in place to provide clarity regarding access to applications outside of Active Directory. Management confirmed that work is underway and in progress to formalise user access for applications. Access requests for additional applications will be managed through IT tickets, but a formalised process under the Cyber Identity Access Management project and is yet to be fully established. The Information Security document is also currently being updated and the user access process is being rewritten.	DESIGN
IMPLICATION	**SIGNIFICANCE**
The outdated Information Security SOP may lead to compliance violations as it does not reflect current best practices and regulatory requirements. Inadequate documentation may impact compliance requirements and the ability to demonstrate effective capacity management practices. The absence of a User Access Management policy and procedure increases the likelihood of inconsistencies in the user access provisioning and deprovisioning processes, leading to operational inefficiencies and delays.	LOW

RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
1. Management should ensure the completion of the review and any updates to the Information Security SOP and finalising the User Access Management policy and procedures.	1. Hazel Irving (on behalf of ISO) and Darrell Gough - UAM	1. Digital Division management acknowledges the auditors' findings: a) Information Management SOP - Work has been progressing in regards to the review and development of the Information Management SOP throughout 2023 and this is currently in the final stages of Consultation (ending 26th April 2024). This will be published by the end of June 2024. Review dates will be added to the policy and added to work plan to ensure the reviews are conducted at the at the appropriate review period. b) A review of UAM Policy will be completed by the end of May 2024 to ensure all areas recommended under Finding 1 are included. Further to this process and procedures will be formalised and expected to be completed by the end of August 2024.	1. Information Management SOP - June 2024. User Access - End of August 2024

DETAILED FINDINGS

RISK: Inadequate oversight of Information Security Standard Operating Procedures (SOP) may lead to inconsistencies and non-compliance.

FINDING 6 - IT POLICIES AND PROCEDURES NOT IN PLACE FOR TWO PROCESSES (CONTINUED)			TYPE
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
2. Continue efforts to formalise user access processes for applications outside of Active Directory, leveraging automation where possible to enhance efficiency and accuracy. 3. Management should develop a formal Capacity Management process document outlining roles, responsibilities, and procedures for monitoring, and reporting resource capacity. The document should be periodically reviewed and updated to reflect any changes in technology, business requirements, and regulatory standards.	2. Joe Carragher 3. Craig Worsley	2. Digital Division management acknowledges the auditors' findings and would refer to Digital Division's ongoing work re: the adoption of the SailPoint Identity Access Management solution that will enable a corporate solution for the management of user access control. 3. Digital Division management acknowledges the auditors' findings and will develop formal capacity management policy and processes. This will be managed through our Document Management Framework and will be subject to annual reviews initiated through workflow.	2. tied to the implementation of IAM / NIAM - June 2025. 3. August 2024

APPENDICES

APPENDIX I: DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
SUBSTANTIAL	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
MODERATE	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
LIMITED	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
NO	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
HIGH	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
MEDIUM	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
LOW	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX II: TERMS OF REFERENCE

EXTRACT FROM TERMS OF REFERENCE

PURPOSE

The purpose of this review is to provide an assessment of the adequacy of the SPA IT General Control environment based on our testing of the design and implementation of key IT controls

KEY RISKS & APPROACH

SCOPE AREA	SUB-AREAS	KEY INHERENT RISKS	APPROACH
IT Governance	IT Strategy	Governance and monitoring measures not in place, leading to an inability for IT to meet SPA objectives.	• Confirm an approved and funded IT Strategy is currently in place with corresponding implementation plans and progress tracking mechanisms. • Verify the existence of relevant artefacts that would support the IT strategy, including: — IT strategy documents. — Minutes or documentation supporting management review and prioritisation activities.
	IT organisation & governance forums	Key IT roles and responsibilities may not be appropriately defined or designated, leading to the IT function not being able to meet SPA requirements.	• Confirm whether IT roles and responsibilities have been formalised and documented. Validate that these positions and roles are in place with key performance measures in place. • Discuss with management the various forums in place to support IT governance (including information security and IT projects) for SPA and verify that periodic meetings are being held and that mitigating actions are being logged and tracked.
	IT policies & procedures	Key IT operational processes are not documented and executed consistently in accordance with SPA's expectations and requirements.	• Discuss the IT policy framework and confirm how IT and relevant staff are made aware of IT policies and procedures. Validate the existence of relevant policies including those encompassing: — Information security — Security incident response plan — User access management — Asset management — Change management — IT incident management — Physical security policy — Backup and recovery.

APPENDIX II: TERMS OF REFERENCE

SCOPE AREA	SUB-AREAS	KEY INHERENT RISKS	APPROACH
IT Governance (contd.)	IT risk management, including information security risks	Risks are not regularly identified and recorded leading to a potential critical IT incident.	• Confirm with management the measures in place to identify, document and monitor IT risks. Verify that mitigating actions raised against risks are being logged and monitored.
Physical Security	Physical access to servers	Unauthorised/inappropriate access to mission critical systems. Inappropriate access to data.	• Confirm with management location of critical servers, communication servers and other offline data storage sites which may host critical data and establish that physical controls / security measures are in place. This may include inspection of third-party assurances (e.g. ISO certification).
User Access	User access provisioning, including movers & leavers	Inappropriate/unauthorised access to data or changes to the system.	• Verify the process in place of how management confirm that users are assigned with the appropriately appropriate access. • Obtain an extract of users from Active Directory list and determine whether accounts are disabled in a timely manner with a limited sample against HR leavers information.
	Privileged access management (PAM)	Inappropriate/unauthorised access to data or changes to the system.	• Confirm the measures that management has in place to monitor accounts with privileged access, including databases and obtain evidence of implementation of these measures.
	Password policies & authentication	Inappropriate/unauthorised access to data or changes to the system.	• Confirm authentication mechanism for selected systems (e.g., SSO, SAML via AD) and how password requirements are being enforced across the organisation. • Obtain the password requirements configured for AD and verify whether these are in line with industry standards. Confirm Single Sign On is enforced for key applications. • Confirm security measures in place, such as multi-factor authentication, to remotely connect to the network.

APPENDIX II: TERMS OF REFERENCE

SCOPE AREA	SUB-AREAS	KEY INHERENT RISKS	APPROACH
Vulnerability Management	Patch Management	Lack of patch management process could lead to the organisation being exposed to security threats or lack of systems/applications functionality.	• Confirm that a patch management policy and processes are in place to monitor and apply patches on key IT infrastructure (Windows OS, Linux OS, laptops, servers and network components). • Confirm whether vulnerability scan results are regularly assessed to determine progress with patching/ vulnerability reduction. • Verify whether critical and high-risk vulnerabilities are added to the organisation's IT risk register or equivalent and risk reporting carried out.
	Penetration Testing	A lack of penetration testing could leave SPA exposed to external security threats.	• Confirm that a penetration testing program has been established and is being maintained. • Confirm that period internal and external penetration tests are being completed in line with a programme or policy. • Verify that identified vulnerabilities are recorded, prioritised, resolved and reported on a periodic basis.
Malware & Traffic Monitoring	Tools & monitoring	Inadequate protections have been put in place to protect internal assets from malicious applications, code, or scripts, leading to a loss of availability of internal assets, or the loss of confidentiality and/or integrity of data residing within these assets	• Confirm with management that irregular traffic/activity monitoring measures in place for SPA and verify the existence and maintenance of tools and software. e.g. anti-virus, IPS, IDS, SIEM, DLP. Verify the existence of a Security Operations Centre ("SOC") or equivalent monitoring and response roles and responsibilities. • Verify that automatic updates for anti-malware signature files has been configured.
IT Security Incident Management	Incident response	Inadequate documentation and controls is in place in relation to security incident response and management mechanisms to be followed may lead to such incidents causing a greater deal of damage.	• Confirm that an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan has been established and maintained. • Verify whether the primary and secondary mechanisms to be used to communicate and report during a security incident are formally established, tested and reviewed on at least an annual basis.
Change Management	Change documentation & approval	Changes may be deployed into the production environment without record and/or approval.	• Confirm whether relevant development and production environments are appropriately segregated for key applications. • Verify with management the segregation of duty measures in place over the development and deployment of system changes into a production environment.

APPENDIX II: TERMS OF REFERENCE

SCOPE AREA	SUB-AREAS	KEY INHERENT RISKS	APPROACH
Change Management **(contd.)**	Testing of change	Changes deployed into production may not be adequately tested, resulting in system downtime or a loss of critical or sensitive data.	• Obtain a list of all changes from the Ivanti system throughout the review period. • To establish implementation, sample one Ivanti change request per type of change to verify that: — Changes were requested, tested and approved in line with policy and CAB requirements. — Evidence of testing (including UAT) and approval are appropriately recorded and maintained.
IT Operations Management	System performance & capacity management	Lack of capacity management on IT systems and application supporting the SPA objectives could result in capacity issues not being identified and remediated in a timely manner, adverse impacting SPA operations.	• Review whether a capacity management policy, and monitoring and alerting processes, are in place and whether these processes are adequately designed. • Verify with management that capacity monitoring and alerting measures are in place on key IT infrastructure. Validate the measures in place to manage capacity issues and incidents identified.
	IT incident & problem management	Management may not be able to track and resolve systems and technology issues that may cause operational disruption.	• Obtain and review the IT Incident management / IT service desk policy and procedure documents and confirm whether SLA's have been established. Assess how management confirm that service requests and IT incident KPIs are in line with SPA's operational requirements. • Obtain an extract of all P1(Critical) incidents from Ivanti though out the audit period. Assess the implementation of the IT incident management process by selecting a sample of one P1(Critical) incident and verify that: — The incident was tracked and resolved in-line with KPIs. — A root cause analysis was performed where applicable.
	Back-up & recovery	Important data may be lost.	• Confirm back-up measures are defined for key systems and critical/sensitive data and whether back-ups are appropriately monitored and tested. • To establish the implementation of backup monitoring, we will select a back-up report where a failure has been identified and assess whether this had been resolved in a timely manner.
	Hardware asset management	Loss of assets or data breach due to insufficient tracking and of inventory and assets.	• Obtain the IT asset register and confirm with management how equipment is tagged, logged, documented and managed. • Validate measures in place to update and monitor the location of equipment.

APPENDIX II: TERMS OF REFERENCE

SCOPE AREA	SUB-AREAS	KEY INHERENT RISKS	APPROACH
IT Operations Management (contd.)	Software asset management	Software licences may be not be utilised, resulting in unnecessary costs. Unlicenced software may result in penalties.	• Confirm with management how the utilisation of software licences are monitored and how SPA prevents the installation of unauthorised software. • Validate that the measures identified are in place.
Third-party Management	Third-party management	Third parties may not meet SPA's internal control requirements, including cyber and data protection.	• Confirm whether an appropriate third-party due diligence process is followed for the onboarding of IT suppliers, with adequate involvement of senior IT management, procurement, compliance, DPO and legal teams. • Confirm that independent assurances on IT controls are available for key suppliers and that a requirement is in place for ongoing supplier monitoring.

APPENDIX II: TERMS OF REFERENCE

SCOPE

The following areas will be covered as part of the scope of this review:

- IT strategy and governance
- Physical security of server environment(s)
- User access, including user provisioning, leavers, privileged access management and password configuration standards
- IT hardware and software asset management
- Vulnerability management
- IT change management
- IT infrastructure performance and capacity management
- Incident and problem management
- Back-up and recovery procedures
- Third-party management.

EXCLUSIONS/LIMITATIONS OF SCOPE

IT risk areas not included in this review include:

- Software development and application controls other than those tests listed in the scope
- Business continuity and IT Disaster Recovery, although the back-up process is included
- Data management and regulatory compliance
- The appropriateness of the current IT strategy
- Programme / project governance and assurance
- Penetration or vulnerability testing procedures.

APPENDIX III : STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.	
Hazel Irving	Head of ICT Service Delivery
David Gillen	IT Lifetime Process Manager
Darrell Gough	Head of IT Operations
Craig Worsley	Head of IT Systems
Colin McLeod	Head of IT Infrastructure
Ian McMillan	Quality Assurance Officer
Richard Allan	Cyber Security and Assurance Manager
Joe Carragher	Head of Applications
Karen Nicol	Procurement Category Manager
Jonathan Clydesdale	Technical Services
Craig Freeland	Technical Services Team Leader
Sheila Macleod	Information Security Officer
Linda Murray	UAM Team

FOR MORE INFORMATION:

JASON GOTTSCHALK, DIGITAL PARTNER

+44 (0) 797 659 7979
jason.gottschalk@bdo.co.uk

CLAIRE ROBERTSON, HEAD OF DIGITAL & RISK ADVISORY SERVICES - SCOTLAND

+44 (0) 7583 237 579
claire.robertson@bdo.co.uk

Disclaimer

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

www.bdo.co.uk

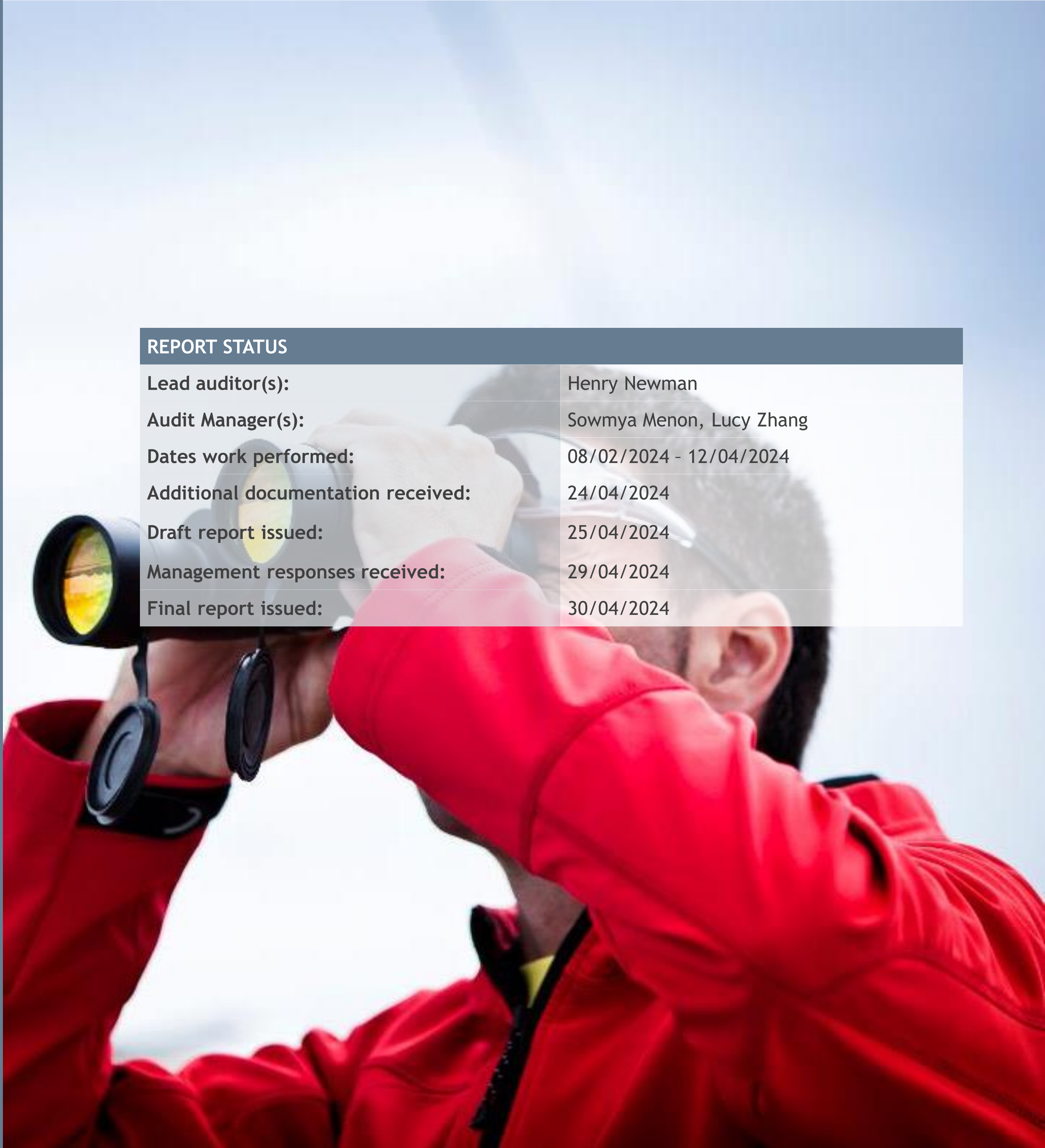
Scottish Police Authority

Best Value Readiness Advisory Review - Final report

April 2024

IDEAS | PEOPLE | TRUST

CONTENTS



REPORT STATUS	
Lead auditor(s):	Henry Newman
Audit Manager(s):	Sowmya Menon, Lucy Zhang
Dates work performed:	08/02/2024 – 12/04/2024
Additional documentation received:	24/04/2024
Draft report issued:	25/04/2024
Management responses received:	29/04/2024
Final report issued:	30/04/2024

RESTRICTIONS OF USE

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

Executive Summary (Page 1 of 2)

Summary of Observations			Agreed actions
H	1	🟥	2
M	1	🟧	2
L	4	🟩🟩🟩	5
TOTAL NUMBER OF Findings: 6			9

Background

Best Value provides a common framework for continuous improvement in public services in Scotland and is a key foundation of the Scottish Government's Public Service Reform agenda.

The Scottish Public Finance Manual (SPFM) outlines that the Scottish Police Authority (SPA or the Authority), Police Scotland, the Chief Constable and Accountable Officer have specific responsibilities to ensure arrangements have been made to secure Best Value. SPFM details they have a duty to:

- "Make arrangements to secure continuous improvement in performance whilst maintaining an appropriate balance between quality and cost; and
- Have regard to economy, efficiency, effectiveness (VFM), the equal opportunities requirements and to contribute to the achievement of sustainable development"

Audit Scotland has an oversight role in respect of Best Value and may choose to undertake an audit of the Scottish Police Authority and Police Scotland's arrangement of achieving Best Value.

HMICS has a statutory duty to enquire into the arrangements made by the Chief Constable and the Authority to meet their obligations in terms of best value and continuous improvement. If necessary, HMICS can be directed by Scottish Ministers to investigate anything relating to the Authority or Police Scotland as they consider appropriate.

Best Value characteristics have been recently regrouped to reflect the key themes which will support the development of an effective organisational context from which public services can deliver key outcomes and ultimately achieve best value:

- Vision and Leadership
- Governance and Accountability
- Use of resources
- Partnership and collaborative working
- Working with Communities
- Sustainability
- Fairness and equality

Scope and approach

The purpose of this review is to provide advice on Best Value assessment readiness in the following areas:

- Alignment with SPFM's key themes;
- Capacity & capability;
- Buy-in;
- Guidance;
- Governance; and
- Continuous Improvement.

During the audit, we had informed discussions with key members of staff and reviewed key documentation to understand and assess the work undertaken by the Authority and Police Force in establishing a Best Value approach and plans going forward on how they will deliver their outcomes.

Executive Summary (Page 2 of 2)

Summary of Observations

The Authority has set out a proposed approach to Best Value assurance in Police Scotland to demonstrate that they are taking appropriate steps to monitor and assess Best Value. A briefing was provided at CMPB resulting in creation of a new role and appointment of a Head of Best Value to lead on this.

A pilot thematic review of Procurement was completed as a proof of concept with a view to use the learnings from this review to inform the development of the Best Value function.

There has been consideration of the team structure that will be required and associated reporting lines. The plan is for force executives to be given the responsibility of completing self-assessments to ensure assessments reflect real-time practices that are adopted on the ground. There are plans in place for regular catch-up meetings to be used as a means for individuals completing the self-assessments to discuss progress and queries with the Best Value team.

There has been consideration of how actions arising from self-assessment will be recorded and monitored using a tool, called 4 Action.

However, the review has highlighted some observations that present risk to the Authority and Police Scotland's approach to Best Value:

- **Resourcing constraints**: There is no clear pathway on how resource requirements will be fulfilled, including feasibility of using additional/external staff to be able to achieve operational delivery of Best Value.
- **Project progress**: There has been no oversight and sign-off on the current status of the project as progress reporting has been paused.

We also identified four further opportunities for improvement. These relate to monitoring of time and resources, the lack of guidance in the form of written procedures/manuals and lack of evidence around use of the 4 Action system to track completion of actions from self-assessments.

Detailed Findings

Detailed Findings

Risk: There may not be adequate capacity and capability to drive the best value self-assessment
Risk: Force Executive may not buy-in to the best value process.

Finding 1 - Resource constraints	Type
The Forward Plan established by the Head of Best Value to demonstrate how to achieve Operational Delivery as BAU by March 2024 is delayed without a clear view on the new timeline. Given the recruitment freeze, the Head of Best Value (BV) has not been able to recruit any permanent staff to fulfil the open positions within the BV team that he has presented to the Force Executive. Short-term resourcing solutions like deployment from a resourcing pool internally and external secondment were considered, but no suitable candidates were identified at the time of writing. During the review, BDO has identified that there is no clear pathway identified by Management on how to fulfil the required resources within the BV team after the recruitment freeze ends, or before. From reviewing all the documents provided by the management, there is no priority assigned to the resourcing requirement for the Best Value team internally.	DESIGN
Implication	**Significance**
This lack of clear pathway identified by the management on how to resource the BV team could lead to operational challenges and may impact the team's ability to deliver on its objectives effectively. It's crucial that a detailed plan is developed to address this gap promptly.	High

Recommendations	Action Owner	Management Response	Completion Date
A new Forward Plan should be developed to reflect realistic progress that the Best Value team can make with current resources, as well as setting out the desired resource level and additional progress that could be made. The updated plan should be agreed with Chief Constable via relevant governance processes.	Head of Best Value	Accepted - A case is to be developed to recruit key team members (up to 4). In addition, the plan is to be updated to reflect the revised timescales for developing training material and commencing the BV assessments	31 August 2024
If additional resources are required to achieve an acceptable level of progress, then management should put a plan in place to identify and secure suitable candidates to ensure operational delivery can be carried out as planned.	Head of Best Value	Accepted - As above, a case will be made to recruit team members. Dates will be revised for the existing plan	30 June 2024

Detailed Findings

Risk: Force Executive may not buy-in to the best value process.

Finding 2 - Progress reporting	Type
Governance and accountability arrangements were identified during the initial Best Value team set up, including: • Chief Constable is the Accountable Officer within Police Scotland. • DCO acts as Senior Responsible Owner for Best Value with CFO acting as depute and line management lead, and a Head of Best Value was appointed. • Best Value Responsible Owners (BVRO) to be identified for individual reviews - aimed at ACC / Director cadre. • Report findings on completed thematic reviews will be provided to CMPB, with escalation up to SLB (as appropriate). • Regular updates may be provided to ARAC for information. We have noted that the Head of the Best Value has a monthly catch up with DCO who acts as Senior Responsible Owner for Best Value and CFO who acts as depute and line management lead to discuss the progress of the plan. However, no formalised meeting minutes have been recorded. The progress reporting was paused to be provided to the governance boards (CMPB (Corporation Management and People Board) and SLB (Senior Leadership Board)) due to the lack of progress made. Given the pause of progress reporting, the delay and slippage of the milestones for the Forward Plan were not monitored effectively to ensure a backup plan was established in a timely manner.	DESIGN
Implication	**Significance**
The continued delay to achieving the project plan put in place for Best Value can result in the organisation failing to demonstrate its effectiveness in operating in accordance with Best Value set out for Police Authorities under Local Government in Scotland Act 2023.	Medium

Recommendations	Action Owner	Management Response	Completion Date
Formalise the governance process around the Best Value projects to ensure sufficient monitoring is in place to ensure the delivery according to the plan agreed. For example, MI reporting pack against agreed plan on the regular basis to accountable officers and relevant boards; any delay of achieving the milestones is discussed with the accountable officers and agree action plan to address such delay.	Head of Best Value	Accepted - While governance has been agreed with the DCO and CMPB, MI will be developed based on experience gained from early assessments. This will include timescales for completion.	31 December 2024
A similar governance process should be considered once the Best Value team is in it BAU operational delivery phase. Regular MI reporting against agreed self-assessment work plans for different teams should be established with the relevant governance boards like CMPB.	Head of Best Value	Accepted - MI will be developed, based on experience from early assessments. This will be improved and linked to outcomes as experience is gained in BAU.	31 December 2024

Detailed Findings

RISK: Contributing departments may not have enough time to complete the self-assessments appropriately.

Finding 3- Monitoring of time and resources	Type
In June 2023, a pilot thematic review of Procurement was completed as proof of concept. This was done with a view to understand time and resource requirements in completing self-assessments to facilitate better planning and decision-making in the implementation of remaining toolkits. While the report prepared by management following the review makes reference to a ‘work plan timetable’ and acknowledges that this was affected by staff absences and year-end financial reporting commitments, there is no evidence of monitoring and reporting of the various stages of the project, such as expected and actual dates of achieving key milestones, time and effort dedicated by staff at different seniority levels, and impact on business-as-usual activities, if any. As such, there is little scope for relevant lessons learnt to be shared with other departments and functions albeit the applicability of lessons would vary in relevance. A Draft Toolkit Workplan has been developed; this lists activities within the Best Value self-assessment cycle, the medium through which these activities would need to be fulfilled (in-person, Teams, etc.), time commitment, dependencies and any related documents and templates. However, during our review we noted the following: • The Workplan does not identify high-level expectations laid out by the Best Value team that are required to be followed-through by individual BVROs. • Of the 16 activities, four activities had no time commitment estimates. • There has been no consideration given to cross-team dependencies that may be relevant for some functions. Furthermore, there is no tracker in place that can be utilised by various teams as a template to develop, record and monitor timelines on an ongoing basis once the self-assessment is initiated.	Design and Effectiveness
Implication	**Significance**
There is a risk that self-assessments require more time commitment than estimated or involve more personnel than initially identified resulting in staff working beyond capacity and/or significant delays in completing self-assessments. In the absence of a tool for monitoring completion of self-assessments on an ongoing basis, there is also a risk that timely action cannot be taken to prevent delays and lessons learnt/good practice cannot be identified.	Low

Recommendations	Action Owner	Management Response	Completion Date
We recommend that: • The Draft Workplan is completed and updated with the Best Value team’s expectations. • A tracker is developed that can be tailored and accessed by various teams to record and monitor timelines on an ongoing basis.	Head of Best Value	Accepted. The workplan for each toolkit, will show high level expected time commitments. This will be augmented by bespoke planning for each toolkit in the introductory training module/workshop to be delivered at the start of each engagement. Although each toolkit/engagement is unique, a tracker will also be developed for each one, to capture actual timescales against plan.	31 December 2024

Detailed Findings

Risk: The self-assessment templates may not clearly demonstrate alignment with the SPFM’s key themes

<table>
<tr><th colspan="3">Finding 4 - Effectiveness of self-assessment</th><th>Type</th></tr>
<tr><td colspan="3">Current guidance on Best Value self-assessment has been referenced under section 8 of the Scottish Public Finance Manual (SPFM). This refreshed guidance revisits the Best Value themes in light of the changing context within which Public Bodies have operated over the last decade. The Best Value in Public Services Guidance for Accountable Officers outlines strategic and operational outcomes under each of the themes that are required to be demonstrated.
The Authority’s current approach to building a framework of self-assessment is centred around 18 toolkits published by Audit Scotland in the past, each of which relates to a specific business area/function. Given that the self-assessment process is still in its infancy, the Authority has not yet tailored 17 of the toolkits to ensure that they not only fit for purpose to be used by the Authority but also consider strategic and operational outcomes expected by the regulator, and other sources of relevant good practice.
Our review of the Authority’s BV Toolkit Analysis spreadsheet showed that there has been a mapping to BV themes. In Appendix I, we have proposed alternate themes for two of the toolkits as these align better in context of the police force and in keeping with the purpose of the themes.</td><td>Design and Effectiveness</td></tr>
<tr><th colspan="3">Implication</th><th>Significance</th></tr>
<tr><td colspan="3">The Authority’s current approach in carrying out self-assessment may not be fully effective in demonstrating compliance with regulatory requirements on Best Value, as the approach is centred around toolkits published by Audit Scotland in the past rather than the Best Value in Public Services Guidance for Accountable Officers.</td><td>Low</td></tr>
<tr><th>Recommendations</th><th>Action Owner</th><th>Management Response</th><th>Completion Date</th></tr>
<tr><td>Self-assessment templates should be developed based on Best Value in Public Services Guidance for Accountable Officers guidance to ensure each of the assessments are current and relevant, considers expected strategic and operational outcomes.
Use of tools such as EFQM would ensure that in each business area, relevant and current best practice is being sought, for example consultation with HR professional bodies for HR areas.</td><td>Head of Best Value</td><td>Accepted. A full review of the toolkits has been undertaken / documented and the 2020 BV themes have all been impacted, together with an impact assessment of Police Scotland risks and strategic priorities. It is agreed that the 7 themes must be tested where appropriate, in all assessments and particularly the cross-cutting themes of sustainability and fairness & equality. These will be built into the toolkits during tailoring prior to each engagement. Initial consideration of an EFQM informed approach took place in December and will be followed up as a priority when resources are available.</td><td>31 December 2024</td></tr>
</table>

Detailed Findings

Risk: There may not be clear guidance in place to support the completion of best value self-assessments

Finding 5 - No formalised written guidance			Type
The Best Value team has not yet developed any written procedures/manuals for the individual teams to access as practical guidance. However, we have noted workshops were conducted by the Best Value team throughout the Procurement self-assessment pilot process to provide support. The root cause of this is due to resourcing constraint as noted in the previous finding.			DESIGN
Implication			Significance
A written procedure/manual can provide easy access reference point for the individual teams when carrying out the self-assessment exercises. This will reduce the repetitive questions from the different part of the organisation for the Best Value team regarding the self-assessment process.			Low
Recommendations	Action Owner	Management Response	Completion Date
Develop relevant written procedures/manual and make it easy to access by the individual teams. This will serve as a reference point for the individual team when completing the Best Value self-assessment.	Head of Best Value	Accepted. The planned development of training material has been well documented in BV planning files. This is seen as critical for embedding a BV culture in the organisation and is anticipated to be developed for 3 complementary purposes. Development of such training material will be a priority for the new team.	31 December 2024

Detailed Findings

Risk: Identified development opportunities may not be implemented.

Finding 6 - Actions tracking			Type
The Best Value team has developed a Tactical Plan to manage service delivery with each of the team. It includes key milestones to complete the team's Best Value self-assessment process. Upon reviewing the Tactical Plan, we do not believe the plan includes key milestone as to how the actions agreed from the self-assessment are followed up and tracked to completion. The tracking system (4 Action) has been identified to be used for tracking actions coming out of the self-assessment process. However, there is no clear plan set out how Management will utilise the tracking system identified (4 Action) effectively to ensure all the actions are tracked to completion. The root cause of this is due to resourcing constraint as noted in the previous finding.			DESIGN
Implication			Significance
There is a risk that actions raised via the self-assessments are not properly tracked and followed up to ensure its timely implementation.			Low
Recommendations	Action Owner	Management Response	Completion Date
Update the Tactical Plan to ensure the key milestones for implementing actions agreed are clearly communicated with the individual teams at the beginning of the self-assessment cycle.	Head of Best Value	Accepted. At the commencement of the engagement, additional emphasis will be placed on the outcomes from the assessment and how these are to be expedited. Follow ups will be scheduled to ensure actions have been effectively expedited in a similar way to Internal Audit actions.	31 December 2024
Formalise the procedures on how to using the 4 Action to tracking the actions. For example, consider how to effectively incorporate the rating system into the 4 Action for the Best Value assessment; utilise the reporting functionality of the system to ensure timely closure of the actions agreed.	Head of Best Value	Accepted - while a rating template has been agreed (as in the pilot), full use of 4-Action and all its functionality will be developed by team members once recruited and trained in the 4 Action product.	31 March 2025

Appendices

Appendix I - Best Value Themes

Toolkit	Current Theme	Proposed Theme	Rationale
Planning Resource Alignment	Effective use of resources	Vision and Leadership	Vision and Leadership**:** Organisations are required to demonstrate that they have a **strategy** with realistic and achievable objectives and targets which are **matched to their financial, asset base and other resources** and which is explicitly translated into clear responsibilities for implementation.
Customer Focus	Vision and leadership	Governance and accountability	In a police context, this would refer to focus on Scotland's people, the local community and how the Authority ensures they are operating in their best interests. Governance and accountability: The organisation has in place appropriate mechanisms for ensuring that it is aware of **citizen, customer, partner and stakeholder views, perceptions, and expectations** so that these can inform its actions.

APPENDIX II: DEFINITIONS

Observation Significance	
High	Presents significant and material risk to one or more of the programme's key time, cost, or quality constraints. There are no clear plans to remediate the risk. OR Represents a specific material issue that has already occurred.
Medium	Represents a risk that has the potential to materially impact one or more of the programme's key time, cost, or quality constraints. The programme is aware and has plans to address but these have not yet brough the risk down to a tolerable level that would indicate a low finding. OR Represents a moderate issue where there is scope to recover time, cost or quality.
Low	There is a likely impact to one or more of the programme's key time, cost, or quality constraints but this is individually within a tolerance that programme management would accept. Low findings need to be considered together for their potential aggregate impact.
Info	Is not likely to have significant impact, but where management may consider a requirement for improved controls and/or can achieve greater effectiveness and/or efficiency of the programme

APPENDIX III: TERMS OF REFERENCE

EXTRACT FROM TERMS OF REFERENCE

PURPOSE

The purpose of this review is to provide advice on Best Value assessment readiness in the following areas:

- Alignment with SPFM's key themes;
- Capacity & capability;
- Buy-in;
- Guidance;
- Governance;
- Continuous Improvement.

KEY RISKS

1. The self-assessment template may not clearly demonstrate alignment with SPFM's key themes
2. There may not be adequate capacity & capability to drive the best value self-assessment
3. Contributing departments may not have enough time to complete the self-assessments appropriately
4. Force executive may not buy-in to the best value process
5. There may not be clear guidance in place to support the completion of best value self -assessments
6. There may not be a clear governance structure in place to monitor best value performance
7. Identified development opportunities may not be implemented.

EXCLUSIONS

The scope of the review is limited to the areas documented under the scope and approach. All other areas are considered outside of the scope for this review.

This is an advisory engagement, as such we will not provide assurance on the control arrangements not the operating effectiveness of these controls. We are reliant on the honest representation by staff and timely provision of information as part of this review.

APPENDIX IV: STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

FULL NAME	JOB TITLE	EXECUTIVE SPONSOR/KEY SPONSOR/Action Owner
Alasdair Corfield	Head of Best Value	Audit Lead
John McNellis	Head of Finance, Audit and Risk	SPA Sponsor
Iain McKie	Head of Strategic Procurement	Key contact
Alan Spiers	DCC Professionalism	PS audit Sponsor
James Gray	Chief Financial Officer	Key Contact
Angela Wood	Head of Policy, Risk, Assurance and Audit	Key contact
Sam Anderson	Business Assurance Manager	Key Contact

APPENDIX V: LIMITATIONS AND RESPONSIBILITIES

MANAGEMENT RESPONSIBILITIES

The Board is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work.

The Board is responsible for ensuring the internal audit function has:

- The support of the organisation's management team.
- Direct access and freedom to report to senior management, including the Chair of the Audit Committee.
- The Board is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the Company.

Internal controls covers the whole system of controls, financial and otherwise, established by the Board in order to carry on the business of the organisation in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The Board is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Board.

LIMITATIONS

The scope of the review is limited to the areas documented under Appendix II - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of colleagues interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

FOR MORE INFORMATION:

Claire Robertson, Director

Claire.Robertson@bdo.co.uk

(Remove FOIA disclosure if your client is not public sector or connected to the government)

[Freedom of Information

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 ("the Act"), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure, and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.]

Disclaimer

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

www.bdo.co.uk