Audit and Risk Assurance Committee

Meeting Date	16 September 2026
Title	Internal audit reports
Author(s)	Nick Atkinson, Head of Internal Audit (RSM) and Sarah Howe, Associate Director (RSM)
Executive Sponsor	Claire Amor, Executive Director of Corporate Affairs

Executive Summary

This report provides the Committee with progress updates on the internal audit plan since the last Audit and Risk Assurance Committee (ARAC meeting in June 2026) and includes any final reports issued and current follow up position. The report has been prepared based on the work performance up to 24 August 2026.

Since the last ARAC meeting, we have issued the following report:

- Incident Management and Business Continuity (Reasonable assurance).

We have also issued the following report in draft:

- Data Quality and Management

Follow Up

There were a total of 37 open actions, consisting of two High, 23 Medium and 12 Low priority management actions. This included those actions handed over from the previous Internal Auditors. Since the last Audit and Risk Assurance Committee meeting;

- Seven (one high, two medium and four low) actions have been implemented, and internal audit have reviewed and validated evidence where required.
- Two medium actions are overdue their original date and management have agreed revised due dates. These relate to the Business Central audit undertaken by BDO and the Incident Management and Business Continuity audit.
- 28 (one high, 19 medium and eight low) actions are not due and will be followed up accordingly when they fall due.

Action required	The Committee is asked to review the information provided and seek clarification on any areas.
Previous consideration	This paper has been presented at the Executive Leadership Team on 1 September 2026.

Next steps	The next report will be received 11 November 2026.
Financial and resource implications	Not applicable.
Associated strategic priority/priorities	Putting patients at the centre of smarter, preventative regulation Supporting healthcare workforce development through proportionate, agile regulation Technology-enabled regulatory excellence and organisational sustainability Strengthening public protection through the regulation of NHS managers
Associated strategic risk(s)	SR05 - HCPC Culture SR09 - Digital Roadmap SR10 - Cyber Security Event SR08 - Financial Sustainability
Risk appetite	Compliance - measured
Communication and engagement	Not applicable.
Equality, diversity and inclusion (EDI) impact and Welsh language standards	Not applicable.
Other impact assessments	Not applicable.
Reason for consideration in the private session of the meeting (if applicable)	Not applicable

Int

THE HEALTH AND CARE PROFESSIONS COUNCIL (HCPC)

Internal Audit Progress Report

16 September 2026

CONTENTS

Appendices

KEY MESSAGES

The internal audit plan for 2026/27 was approved by the Audit and Risk Assurance Committee at the 11 March 2026 meeting. This report provides an update on progress against the plan and summarises the results of our work to date.

Internal Audit Plan 2026/27
Since the last meeting, we have finalised the Incident Management and Business Continuity report and issued a **reasonable assurance** opinion.

The draft report for the Data Quality and Management audit has been issued. The fieldwork for the Corporate Complaints is currently in progress.

Further details of the progress made against the internal audit plan are included in **Appendix A**. **[To discuss and note]**

Additional Review – Key Performance Indicators

At the request of management, RSM completed a separate review around key performance indicators. A workshop has taken place, and the work has now concluded. **[For information]**

Follow Up of Management Actions
As part of the new follow up process, RSM now undertakes the ongoing follow up of previously agreed management actions. We have included the details of this follow up, within this paper. There was a total of 37 open actions, consisting of two High, 23 Medium and 12 Low priority management actions. This included those actions handed over from the previous Internal Auditors. Since the last Audit and Risk Assurance Committee meeting;

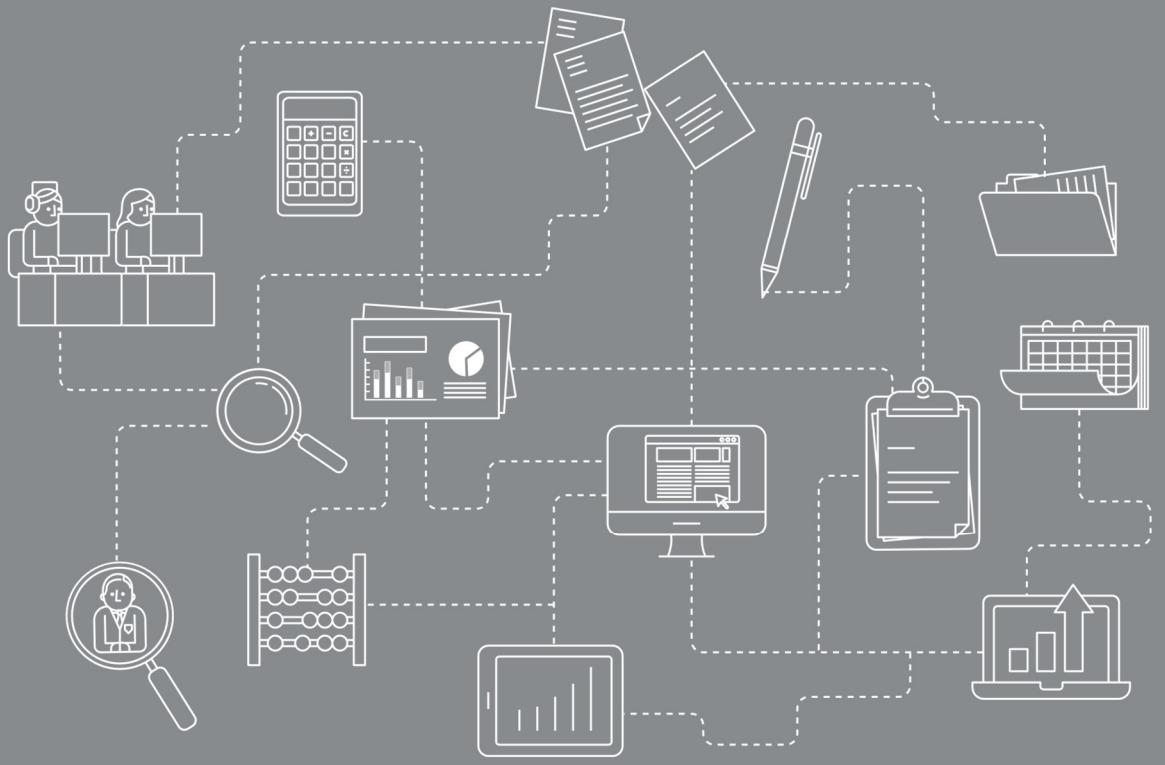
- Seven (one high, two medium and four low) actions have been implemented, and internal audit have reviewed and validated evidence where required.
- Two medium actions are overdue their original date and management have agreed revised due dates. These relate to the Business Central audit undertaken by BDO and the Incident Management and Business Continuity audit.
- 28 (one high, 19 medium and eight low) actions are not due and will be followed up accordingly when they fall due.

Please refer to section 1.4 and Appendix B for further detail. [To approve]

Progress Meetings
We have scheduled progress meetings with the Head of Assurance and Compliance on a quarterly basis regarding delivery against the Internal Audit Plan. **[To note]**

Final Reports

01



1. FINAL REPORTS

1.1 Summary of final reports being presented to this Committee

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

Assignment	Opinion issued	Actions agreed			
		A	L	M	H
Incident Management and Business Continuity Overall, the HCPC has established key elements of a business continuity framework, including business continuity and emergency response plans, risk assessments, and arrangements for reporting incidents and testing outcomes. However, further improvements are required to clarify incident escalation and de-escalation responsibilities, strengthen training and risk-based testing arrangements, and ensure lessons learned from incidents and test exercises are consistently shared across the organisation to support continuous improvement. At the time of our review, it was noted that responsibility for business continuity has largely resided with the Chief Information Security Risk Officer, and the departure of the postholder presents a risk to continuity of ownership and oversight. Addressing these areas will improve resilience and enhance the HCPC's ability to respond effectively to disruptions.	Reasonable Assurance	0	2	4	0

1.2 Themes arising from control observations

Theme	Advisory	Low	Medium	High
Governance Weakness		1	-	-
Policies and procedures		-	2	-
Training / awareness for staff		-	1	-
Planning		-	1	-
Poor record keeping		1	-	-
Total		**2**	**4**	**-**

We do not have any concerns in respect of themes arising to raise with the Committee at this stage.

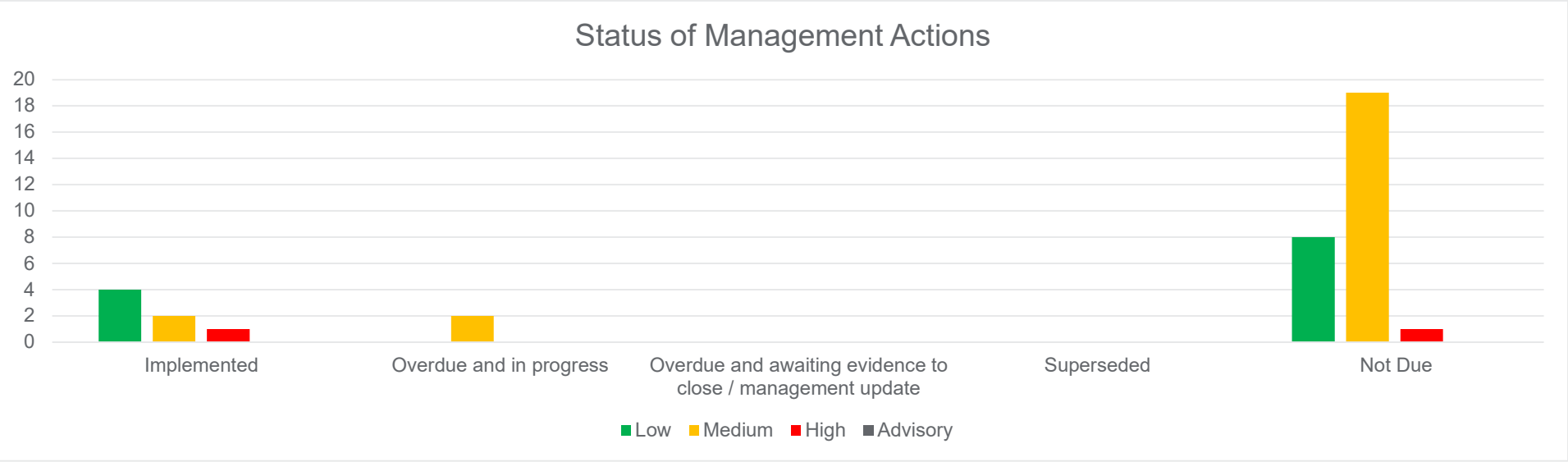
1.3 Follow up

In order to meet the Chartered Institute of Internal Auditors (CIIA) Standards and to provide management with assurance regarding the implementation of agreed actions, Internal Audit has undertaken a follow-up exercise to determine the status of outstanding management actions that have become due for implementation. In assessing the implementation of agreed actions Internal Audit has:

- Contacted all responsible managers within the organisation requesting a status update and supporting evidence in respect of the actions in their areas.
- Reviewed all supporting evidence in order to provide an independent viewpoint regarding whether each action was fully implemented, being implemented or not implemented at all.

There was a total of 37 open actions, consisting of two High, 23 Medium and 12 Low priority management actions. This included those actions handed over from the previous Internal Auditors. Since the last Audit and Risk Assurance Committee meeting;

- Seven (one high, two medium and four low) actions have been implemented, and internal audit have reviewed and validated evidence where required.
- Two medium actions are overdue their original date and management have agreed revised due dates. This relates to the Business Central audit undertaken by BDO and the Incident Management and Business Continuity audit.
- 28 (one high, 19 medium and eight low) actions are not due and will be followed up accordingly when they fall due.



Refer to Appendix B for further information.

Those lines shaded green, indicate audits where management actions are now fully implemented and therefore will not appear in future iterations of this paper.

Implementation status by review	TOTAL	Implemented	Overdue and in progress	Not implemented	Superseded	Not applicable	Not yet due
Business Central	5	1	1	-	-	-	3
Cyber Security	2	-	-	-	-	-	2
Diversity	1	1	-	-	-	-	-
Environmental Sustainability	2	-	-	-	-	-	2
Health and Safety	3	-	-	-	-	-	3
KPIs	3	3	-	-	-	-	-
Outreach	2	-	-	-	-	-	2
Procurement of Large Contracts	2	-	-	-	-	-	2
Stakeholder Engagement	1	-	-	-	-	-	1
Risk Management	8	-	-	-	-	-	8
Follow Up Audit	2	1	-	-	-	-	1
Incident Management and Business Continuity	6	1	1	-	-	-	4
Total	**37**	**7**	**2**	**-**	**-**	**-**	**28**

Appendices

02

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

Assignment and Executive Lead	Status / Opinion issued	Actions agreed				Target Committee meeting (as per IA plan / change controls*)	Actual Committee meeting
		A	L	M	H		
Incident Management and Business Continuity **Claire Amor - Executive Director of Corporate Affairs**	**Final** **Reasonable Assurance**	**0**	**2**	**4**	**0**	**June 2026**	**September 2026**
Data Quality and Management Andrew Smith - Deputy CEO and Executive Director of ERRS	Draft report issued 18 August – awaiting response. *Short delay in issuing this report, due to annual leave.*	-	-	-	-	September 2026	
Corporate Complaints Claire Amor - Executive Director of Corporate Affairs	Fieldwork in progress	-	-	-	-	December 2026	
Key Financial Controls - Accounts Receivables / Registration Fees Alastair Bridges - Executive Director of Resources	Scoping – proposed to start in November 2026.	-	-	-	-	March 2027	

APPENDIX B: INTERNAL AUDIT ACTIONS

The following actions are overdue with a revised due date.

Report Name	Audit Management Action	Priority	Action Owner	Executive Lead	Due Date	Status
Business Central	HCPC should determine if it prefers to have an overarching Financial Regulations document which cross references to detailed procedure documents, or detailed financial manual with all procedures included (a similar finding has been made previously). Regardless of approach, the gaps in procedures identified should be addressed, including adding reference to BC as the finance system in use.	**Medium**	Aihab Al Koubasi, Financial Controller	Alastair Bridges - Executive Director of Resources	31 March 2026 16 September 2026 (ARAC) **Revised due date: 30 November 2026**	**Action in progress – revised due date agreed.** The first draft of the Finance Manual was submitted on 24 March 2026. This manual consolidates and documents all items that were recommended by the Internal Auditors. The finance manual incorporates the scheme of delegation, financial regulations and all the policies and procedures. The Finance Manual has not yet been approved by ARAC. The Finance Manual will be presented to ARAC on Wednesday, 11 November 2026.
Incident Management and Business Continuity	Processes relating to scenario testing, post incident reviews and escalation and de-escalation of plans will be documented in the Business Continuity Strategy.	**Medium**	Emmanuel Ogungbe - Information Governance and Risk Lead	Claire Amor - Executive Director of Corporate Affairs	31 July 2026 **Revised due date: 31 October 2026**	**Action in progress – revised due date agreed.** A strategy / policy document has been drafted covering the points highlighted. Any changes will be made by the Information Governance & Risk Lead. This will go to the Information & Technology Governance Board Meeting, and ELT for note.

APPENDIX C: OTHER MATTERS

External Quality Assessment

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

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

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

- We will commission an external assessor to perform a review of the design of our internal audit methodology, and arrangements to meet the GIAS. The review will cover all 15 Principles and 52 Standards across the Domains of the GIAS, from a design perspective.
- The review will also assess our alignment with the Chartered IIA Internal Audit Code of Practice.
- Following the assessment, RSM will receive detailed feedback and will share a high-level conformance statement of the results with clients.

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

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

Quality assurance and continual improvement

To ensure that RSM remains compliant with the Global Internal Audit Standards in the UK Public Sector we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews are used to inform the training needs of our audit teams.

As part of the Quality Assessment and Improvement Programme, none of your files were selected for Internal Quality Monitoring programme during 2026/27. From the results of the reviews undertaken across our client base, there are no areas which we believe warrant flagging to your attention as impacting on the quality of the service we provide to you.

In addition to this, any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments is also taken into consideration to continually improve the service we provide and inform any training requirements.

Post assignment surveys

We are committed to delivering an excellent client experience every time we work with you. Your feedback helps us to improve the quality of the service we deliver to you. Following the completion of each product, we include a link to a brief survey in each report we issue.

We are committed to delivering an excellent client experience every time we work with you. Your feedback helps us to improve the quality of the service we deliver to you. Currently, following the completion of each product we deliver we attached a brief survey for the client lead to complete. We would like to give you the opportunity to consider how frequently you receive these feedback requests; and whether the current format works. Options available are:

- After each review (current option).
- Monthly / quarterly / annual feedback request.
- Executive lead only, or executive lead and key team members.

APPENDIX D: KEY PERFORMANCE INDICATORS

Delivery				Quality			
	Target	Actual	Notes*		Target	Actual	Notes*
Audits commenced in line with original timescales*	Yes	Yes		Conformance with the Global Internal Audit Standards in the UK Public Sector	Yes	Yes	
Draft reports issued within 10 days of debrief meeting	10 days	1 / 2 (50%)	1	Liaison with external audit to allow, where appropriate and required, the external auditor to place reliance on the work of internal audit	Yes	Yes	
Management responses received within 10 days of draft report	10 days	0 / 1 (0%)	2	Response time for all general enquiries for assistance	2 working days	2 days	
Final report issued within 3 days of management response	3 days	1 / 1 (100%)		Response for emergencies and potential fraud	1 working day	1 day	

Note 1: There was a short delay of 7 days issuing the draft report for the Data Quality and Management audit due to planned leave over summer.

Note 2: We encountered delays in receiving management responses in relation to the Incident Management and Business Continuity report.

Notes
This takes into account changes agreed by management and Audit Committee during the year. Through employing an agile or a flexible approach to our service delivery we are able to respond to your assurance needs.

FOR FURTHER INFORMATION CONTACT

Nick Atkinson, Head of Internal Audit

Email: Nick.Atkinson@rsmuk.com
Phone: +44 (0) 20 3201 8028

Sarah Howe, Associate Director

Email: Sarah.Howe@rsmuk.com
Telephone: +44 (0) 203 201 8773

Clara Agyekumhene, Managing Consultant

Email: Clara.Agyekumhene@rsmuk.com
Telephone: +44 (0) 20 3201 8797

AUDIT OUTCOME OVERVIEW – INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

Background: An audit of Incident Management and Business Continuity was undertaken at the Health and Care Professions Council (the HCPC) as part of the 2026/27 Internal Audit Plan.

There is a Business Continuity Strategy in place which states that there are two types of business continuity events which can impact the HCPC:

1. Fire, flood or pandemic including loss of physical access to the main buildings used by staff every day.
2. Information technology based issues.

The Chief Information Risk and Security Officer is responsible for business continuity at the HCPC. There is a Business Continuity Plan (BCP) in place which is supported by an Emergency Response Plan. These documents detail the roles and responsibilities for business continuity if an incident were to arise.

The BCP can be accessed remotely through ShadowPlanner, which is an online and mobile phone based application. This includes key processes for use in an emergency. The App is accessible to those with line management or business continuity responsibilities.

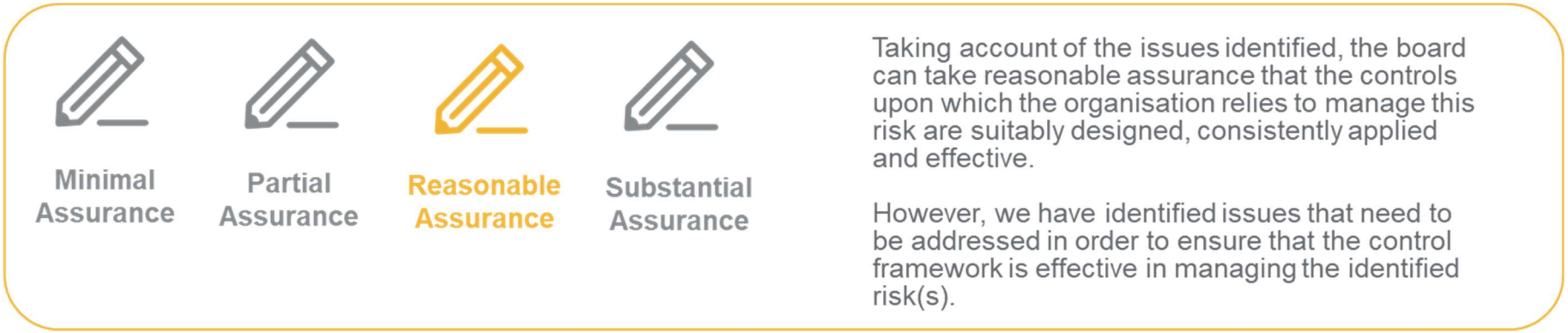
In the last 12 months, there have been no business continuity incidents. Management informed that the last incident occurred in March 2023.

Conclusion: Overall, the HCPC has established key elements of a business continuity framework such as a Business Continuity Plan, Emergency Response Plan, and risk assessment processes. A process is in place for reporting on testing activities and incidents, through which lessons learned are identified and communicated to Heads of Departments. However, responsibility for business continuity has primarily resided with the CISRO, whose impending retirement departure presents a potential risk to continuity of ownership and oversight.

Whilst our audit identified that there are processes and a strategy in place to support the Business Continuity Plan, we noted that further clarity is required around the roles and responsibilities for escalating and de-escalating incidents as well as structured training and risk-based testing. Additionally, it was not clear whether learning from incidents and tests are shared wider across the organisation which reduces the effectiveness of continuous improvement.

We acknowledge that the HCPC is a hybrid organisation and a large proportion of staff work remotely. However, improvements are required to be made to enhance the control framework, otherwise there may be a risk that the organisation may not respond effectively to disruptions. Strengthening governance, formalising processes, and embedding a more structured and proactive approach will significantly enhance resilience and business continuity capability.

Internal audit opinion:



Audit themes:

From our review, we have raised four medium and two low priority management actions, Further details, including detail around the low priority action, can be found in Section 2 of the report.

Business Continuity Plan (BCP)

There is a Business Continuity Plan (BCP) in place which outlines roles and responsibilities and details triggers and actions relating to a range of disruption scenarios. However, review noted that the Plan does not specify the processes and requirements for regular formalised scenario testing (although we note some testing is undertaken), post incident and exercise reporting. Whilst the strategy states that the Plan should be reviewed annually and individual plans should be reviewed every six months, it was not clear when the last review took place.

There is a risk that employees are not aware of key processes relating to business continuity arrangements and therefore are unable to respond accordingly if there was an incident. (**Medium – Management Action 1)**

Roles and Responsibilities

Review of the plan noted that the roles and responsibilities for escalating and de-escalating incidents was not clearly outlined and there was no reference to key individuals involved in these processes. A lack of defined escalation ownership increases the risk of delayed decision-making and ineffective incident response. (**Medium – Management Action 1)**

Training

Currently there is no structured training programme in place for heads of departments and staff. Training is provided through learning identified through incidents and tests, or during ad-hoc workshops. A lack of formal training increases the risk of ineffective incident response and disruption to critical services. (**Medium – Management Action 3)**

Testing of the Business Continuity Plan

Whilst management informed us that testing of scenarios is undertaken on a three year cycle, there was no evidence of a testing plan or equivalent to confirm that all business areas are tested over this period. Similarly, it was not clear whether testing of business areas is risk assessed to identify which tests should be prioritised based on the associated risks.

A lack of a risk-based testing plan increases the risk that key business areas may not be tested, leading to an ineffective business continuity response. (**Medium – Management Action 4)**

Sharing of Learning

Recommendations are raised and management responses are provided in reports following the investigations. However, we noted that whilst responsible owners had been agreed, due dates were not assigned. Furthermore, whilst learning is identified and documented in reports following test scenarios and incidents, there was no evidence provided to confirm that learning was triangulated across the organisation and presented to the Executive Leadership Team or Audit and Risk Assurance Committee. Where learning is identified and not triangulated across the organisation, there is a risk that learning identified from business continuity tests or incidents is not effectively embedded in the organisation, which in turn could reduce resilience to future incidents. (**Medium – Management Action 6)**

Oversight for Business Continuity Arrangements

Discussion with management informed us that there is currently no governance group or committee that has oversight of business continuity arrangements. On an ad-hoc basis or where required, serious incident reports may be presented to the Executive Leadership Team (ELT) for discussion, however this is not on a consistent basis. This could lead to a risk of unclear ownership, inadequate oversight and missed opportunities to share learning from incidents. (**Medium – Management Action 6)**

Notwithstanding the above, we have identified the following instance of good control:

Emergency Response Plan

There is an Emergency Response Plan in place which provides guidance for responding to different types of emergency situations. This includes building and facilities issues, lift entrapment, fire, power outage, medical responses, regulatory incidents, security issues, cyber security incidents, pandemic responses, evacuation for disabled individuals and mass casualty and crisis management. Further review of the ERP confirmed that the roles and responsibilities of key stakeholders at the HCPC are outlined as well as emergency contacts. There is an Incident, Event Evacuation and Invacuation Record sheet template and a Post Evacuation Debrief form which supports the ERP.

Business Continuity Strategy

There is a Business Continuity Strategy in place dated June 2025 which provides an overview of the business continuity arrangements in place at the HCPC. The strategy outlines the aims and objectives of the Plan, responsibility for business continuity, training and review processes.

Risk Assessments

The Business Continuity Strategy states that business impact analyses (BIAs) are completed and are recorded in the Risk Info Assets spreadsheet. This is used to develop the Plan. A walkthrough was performed at the time of our audit due to the confidential information contained in the document. The Info Assets Spreadsheet is maintained by the Risk and Compliance department and lists all the information assets for the ISO27001 accreditation. Each information asset identified is risk assessed with respect to confidentiality, integrity and availability, and a score is recorded.

Key details are also recorded relating to Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Maximum Tolerable Period (MTP) of Disruption and Recovery Time for Provision of Data (RTPD). Further review noted that the spreadsheet covers departments, hard copy records, risk assets, traditional assets and people (although people are not risk scored). The spreadsheet is reviewed annually by the CISRO and evidence of the audit trail log was reviewed.

Reporting of Incidents

At the time of our audit, management informed that there had been no business continuity incidents in the last 12 months. Management informed the last business continuity incident was in March 2023. An Event Reporting Form was completed by the Head of Facilities and included the location of the event, date of event, type of event, key details and any immediate action taken (if required). A Serious Events Report was completed by the CISRO and signed off by the Head of Facilities. Review of the SER confirmed that the methodology, findings and recommendations were outlined. Recommendations were supported by a detailed action plan. Although, it was noted that actions were not assigned due dates.

Serious Event Report – Testing of the BCP

A report is in place for a test completed for the Communications Function in March 2026. Review of the report confirmed that the methodology and findings were outlined along with an action plan. Further review noted that the report was signed off by the Head of Comms, Engagement and Public Affairs.

Another example of a test scenario completed was provided for the Hearings Team and the findings were accepted in July 2025. Review of the report confirmed that an assurance rating was reported and recommendations were raised. The report was completed by the CISRO and signed off by the Operational Manager - Hearings. Further review of the report noted that methodology and findings were outlined and recommendations were recorded in an action plan.

SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

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

Ref	Action	Priority	Responsible Owner	Date
1	Processes relating to scenario testing, post incident reviews and escalation and de-escalation of plans will be documented in the Business Continuity Strategy.	Medium	Chief Information Security & Risk Officer	31/07/2026
2	All reviews of the BCP will be documented with evidence of approval by appropriate stakeholders. The next review date will also be recorded in the Plan.	Low	Information Governance & Risk Lead	31/03/2027
3	Training will be provided to staff on a periodic basis in relation to the business continuity arrangements and a record of attendance will be maintained. Any learning identified from incidents and testing of incidents will be incorporated into the cyclical training programme. *Management response:* *Training relating to BCM / DR for general employees will be via the Corporate Induction process and the annual Information Security & Compliance training provided.*	Medium	Information Governance & Risk Lead	29/01/2027
4	Agree a three-year test programme for the business continuity plan. Business areas will be risk assessed and this will be used to inform the timings of testing for each business area.	Medium	Information Governance & Risk Lead	31/03/2027
5	The incident log will be updated to categorise incidents by type.	Low	Chief Information Security & Risk Officer	31/07/2026
6	At agreed intervals, the Information Security and Compliance Group and / or the Information and Technology Governance Board will provide assurance to the Senior Leadership Team (SLT) or Executive Leadership Team (ELT) on business continuity arrangements. This will include the progress made to implement recommendations and actions as well as learning identified from business continuity incidents and tests which have been conducted. *Management response:* *Although a Serious Event Report may be produced for some serious incidents, all learning will be captured in the Improvement Log.*	Medium	Information Governance & Risk Lead	31/03/2027

External Quality Assessment | June 2026

Purpose and regulatory requirements

RSM UK operates in accordance with the Global Internal Audit Standards, as issued by The Institute of Internal Auditors (IIA). The standards require internal audit to undertake an External Quality Assessment (EQA) at least once every five years. RSM last commissioned an external independent review of its internal audit services in 2021 where we achieved "generally conforms" the highest standard awarded. Our next EQA is scheduled to commence in October 2026.

An EQA provides independent, objective assurance that our internal audit services are delivered in conformance with professional standards and leading practice. The EQA assesses quality, effectiveness and consistency to provide assurance that internal audit continues to support the governance, risk management and internal control needs of our clients. The EQA complements, but does not replace, our internal quality processes.

Since our last EQA, the IIA has issued new standards, effective from January 2025. The new Global Internal Audit Standard 8.4 states that:

"The chief audit executive must develop a plan for an external quality assessment and discuss the plan with the board. The external assessment must be performed at least once every five years by a qualified, independent assessor or assessment team."

This briefing summarises our approach to EQA and is intended to support discussions with the board / audit committee and senior management.

Multi-client providers of internal audit

RSM delivers outsourced internal audit services to a wide range of clients across the public, private, not for profit, and financial services sectors. As such, RSM is classified as a multi-client provider (MCP).

The Global Internal Audit Standards (GIAS) place enhanced responsibilities on the Chief Audit Executive (CAE). Many of the requirements assume the CAE, often referred to as the Head of Internal Audit (HoIA), has the organisational standing, access, and influence typically associated with an employee, in an in-house role.

The standards elevate the role of internal audit and strengthen requirements for effective Quality Assurance and Improvement Programmes (QAIP), an approach already embedded into our processes and operating model. However, the Essential Conditions in Domain III: Governing the Internal Audit Function, introduce specific responsibilities for the board / audit committee and senior management needed for internal audit to operate effectively. These responsibilities are outside of the control of an MCP and the arrangements will vary between organisations. There are also contractual confidentiality matters to consider and the potential for unplanned costs not factored into existing contracts.

Global Internal Audit Standards: Five Domains

Domain I
- Purpose of Internal Auditing

Domain II
- Ethics and Professionalism

Domain III
- Governing the Internal Audit Function

Domain IV
- Managing the Internal Audit Function

Domain V
- Performing Internal Audit Services

The Chartered Institute of Internal Auditors (Chartered IIA) recognises that the GIAS introduce practical challenges for MCPs delivering outsourced internal audit services, particularly in relation to the Essential Conditions. These considerations must be reflected in the approach to EQA.

Our chosen approach

Chartered IIA guidance acknowledges that EQA approaches for MCPs should be proportionate and tailored in scope, recognising that it is not feasible to fully assess all GIAS requirements at the service provider level. Our approach to EQA follows guidance from the Chartered IIA for MCPs.

- We will commission an "external assessor to perform a review of the design of the arrangements in place to meet the GIAS." The assessment will focus on our internal audit methodology, processes and the overall assurance on conformance will be limited to whether our arrangements are designed, in general, to meet the requirements of GIAS. The EQA will cover all 15 Principles, and 52 Standards across the Domains of the GIAS, from a design perspective.
- Our EQA will review the design of our arrangements to meet the requirements of the UK Public Sector Application Note.
- To review our alignment with the Chartered IIA Internal Audit Code of Practice and for clients that have an individual audit plan exceeding 500 days the EQA will encompass file sampling and client interviews.
- Following the assessment, we will receive detailed feedback and will share a high-level summary statement of the results with clients. Where our arrangements are assessed as designed to achieve conformance with the standards, it should be noted that for "Domain III [Governing the Internal Audit Function] the overall achievement remains dependent on the arrangements in place for each client."

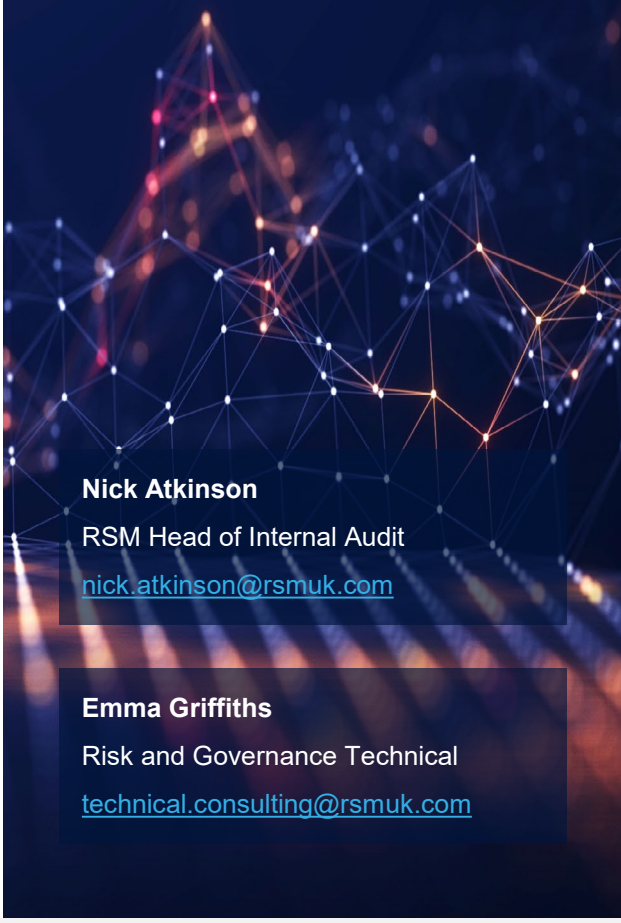
QAIP and next steps

We have a mature QAIP, encompassing internal assessments undertaken by our Quality Assurance Department, periodic self-assessments, clear performance metrics and regular reporting. Undertaking an EQA demonstrates our continued commitment to quality, professional standards, and continual improvement. Our approach is proportionate, aligned to the standards and Chartered IIA guidance for MCPs. It is tailored to the scale of the service we provide, ensuring the scope and form of the EQA remain risk-based, while providing appropriate independent assurance to stakeholders.

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

Further information

- Chartered Institute of Internal Auditors "External Quality Assessment (EQA) – multi client providers"
- RSM "Global Internal Audit Standards, Key Stakeholder Requirements"
- RSM "Quality Assurance and Improvement Programme"
- For copies of RSM briefings please speak to your usual RSM internal audit contact.



Nick Atkinson
RSM Head of Internal Audit
nick.atkinson@rsmuk.com

Emma Griffiths
Risk and Governance Technical
technical.consulting@rsmuk.com

THE HEALTH AND CARE PROFESSIONS COUNCIL (HCPC)

Incident Management and Business Continuity

FINAL Internal Audit Report: 1.26/27

6 July 2026

CONTENTS

Appendices

AUDIT OUTCOME OVERVIEW

In line with our scope, included at Appendix C, the overview of our findings is detailed below.

Background: An audit of Incident Management and Business Continuity was undertaken at the Health and Care Professions Council (the HCPC) as part of the 2026/27 Internal Audit Plan.

There is a Business Continuity Strategy in place which states that there are two types of business continuity events which can impact the HCPC:

1. Fire, flood or pandemic including loss of physical access to the main buildings used by staff every day.
2. Information technology based issues.

The Chief Information Risk and Security Officer is responsible for business continuity at the HCPC. There is a Business Continuity Plan (BCP) in place which is supported by an Emergency Response Plan. These documents detail the roles and responsibilities for business continuity if an incident were to arise.

The BCP can be accessed remotely through ShadowPlanner, which is an online and mobile phone based application. This includes key processes for use in an emergency. The App is accessible to those with line management or business continuity responsibilities.

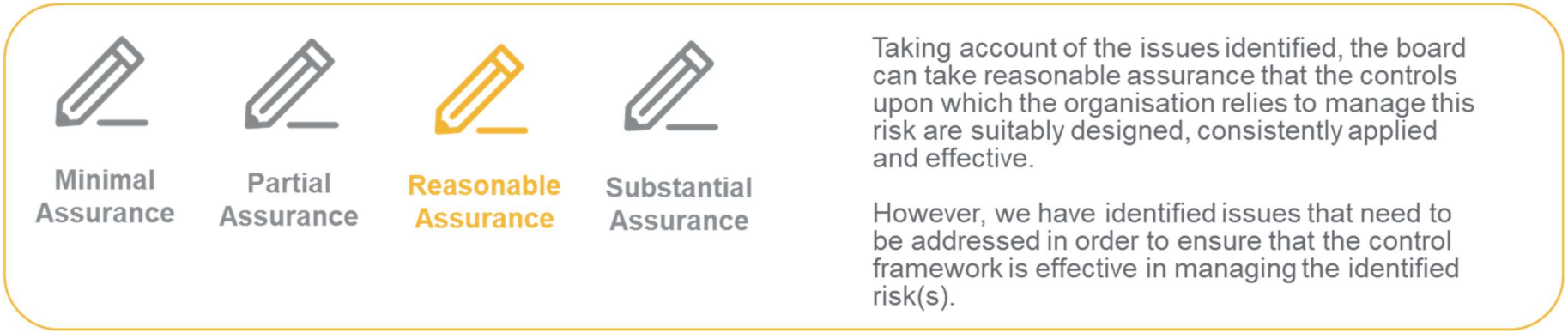
In the last 12 months, there have been no business continuity incidents. Management informed that the last incident occurred in March 2023.

Conclusion: Overall, the HCPC has established key elements of a business continuity framework such as a Business Continuity Plan, Emergency Response Plan, and risk assessment processes. A process is in place for reporting on testing activities and incidents, through which lessons learned are identified and communicated to Heads of Departments. However, responsibility for business continuity has primarily resided with the CISRO, whose impending retirement departure presents a potential risk to continuity of ownership and oversight.

Whilst our audit identified that there are processes and a strategy in place to support the Business Continuity Plan, we noted that further clarity is required around the roles and responsibilities for escalating and de-escalating incidents as well as structured training and risk-based testing. Additionally, it was not clear whether learning from incidents and tests are shared wider across the organisation which reduces the effectiveness of continuous improvement.

We acknowledge that the HCPC is a hybrid organisation and a large proportion of staff work remotely. However, improvements are required to be made to enhance the control framework, otherwise there may be a risk that the organisation may not respond effectively to disruptions. Strengthening governance, formalising processes, and embedding a more structured and proactive approach will significantly enhance resilience and business continuity capability.

Internal audit opinion:



Audit themes:

From our review, we have raised four medium and two low priority management actions, Further details, including detail around the low priority action, can be found in Section 2 of the report.

Business Continuity Plan (BCP)

There is a Business Continuity Plan (BCP) in place which outlines roles and responsibilities and details triggers and actions relating to a range of disruption scenarios. However, review noted that the Plan does not specify the processes and requirements for regular formalised scenario testing (although we note some testing is undertaken), post incident and exercise reporting. Whilst the strategy states that the Plan should be reviewed annually and individual plans should be reviewed every six months, it was not clear when the last review took place.

There is a risk that employees are not aware of key processes relating to business continuity arrangements and therefore are unable to respond accordingly if there was an incident. (**Medium – Management Action 1)**

Roles and Responsibilities

Review of the plan noted that the roles and responsibilities for escalating and de-escalating incidents was not clearly outlined and there was no reference to key individuals involved in these processes. A lack of defined escalation ownership increases the risk of delayed decision-making and ineffective incident response. (**Medium – Management Action 1)**

Training

Currently there is no structured training programme in place for heads of departments and staff. Training is provided through learning identified through incidents and tests, or during ad-hoc workshops. A lack of formal training increases the risk of ineffective incident response and disruption to critical services. (**Medium – Management Action 3)**

Testing of the Business Continuity Plan

Whilst management informed us that testing of scenarios is undertaken on a three year cycle, there was no evidence of a testing plan or equivalent to confirm that all business areas are tested over this period. Similarly, it was not clear whether testing of business areas is risk assessed to identify which tests should be prioritised based on the associated risks.

A lack of a risk-based testing plan increases the risk that key business areas may not be tested, leading to an ineffective business continuity response. (**Medium – Management Action 4)**

Sharing of Learning

Recommendations are raised and management responses are provided in reports following the investigations. However, we noted that whilst responsible owners had been agreed, due dates were not assigned. Furthermore, whilst learning is identified and documented in reports following test scenarios and incidents, there was no evidence provided to confirm that learning was triangulated across the organisation and presented to the Executive Leadership Team or Audit and Risk Assurance Committee. Where learning is identified and not triangulated across the organisation, there is a risk that learning identified from business continuity tests or incidents is not effectively embedded in the organisation, which in turn could reduce resilience to future incidents. (**Medium – Management Action 6)**

Oversight for Business Continuity Arrangements

Discussion with management informed us that there is currently no governance group or committee that has oversight of business continuity arrangements. On an ad-hoc basis or where required, serious incident reports may be presented to the Executive Leadership Team (ELT) for discussion, however this is not on a consistent basis. This could lead to a risk of unclear ownership, inadequate oversight and missed opportunities to share learning from incidents. (**Medium – Management Action 6)**

Notwithstanding the above, we have identified the following instance of good control:

Emergency Response Plan

There is an Emergency Response Plan in place which provides guidance for responding to different types of emergency situations. This includes building and facilities issues, lift entrapment, fire, power outage, medical responses, regulatory incidents, security issues, cyber security incidents, pandemic responses, evacuation for disabled individuals and mass casualty and crisis management. Further review of the ERP confirmed that the roles and responsibilities of key stakeholders at the HCPC are outlined as well as emergency contacts. There is an Incident, Event Evacuation and Invacuation Record sheet template and a Post Evacuation Debrief form which supports the ERP.

Business Continuity Strategy

There is a Business Continuity Strategy in place dated June 2025 which provides an overview of the business continuity arrangements in place at the HCPC. The strategy outlines the aims and objectives of the Plan, responsibility for business continuity, training and review processes.

Risk Assessments

The Business Continuity Strategy states that business impact analyses (BIAs) are completed and are recorded in the Risk Info Assets spreadsheet. This is used to develop the Plan. A walkthrough was performed at the time of our audit due to the confidential information contained in the document. The Info Assets Spreadsheet is maintained by the Risk and Compliance department and lists all the information assets for the ISO27001 accreditation. Each information asset identified is risk assessed with respect to confidentiality, integrity and availability, and a score is recorded.

Key details are also recorded relating to Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Maximum Tolerable Period (MTP) of Disruption and Recovery Time for Provision of Data (RTPD). Further review noted that the spreadsheet covers departments, hard copy records, risk assets, traditional assets and people (although people are not risk scored). The spreadsheet is reviewed annually by the CISRO and evidence of the audit trail log was reviewed.

Reporting of Incidents

At the time of our audit, management informed that there had been no business continuity incidents in the last 12 months. Management informed the last business continuity incident was in March 2023. An Event Reporting Form was completed by the Head of Facilities and included the location of the event, date of event, type of event, key details and any immediate action taken (if required). A Serious Events Report was completed by the CISRO and signed off by the Head of Facilities. Review of the SER confirmed that the methodology, findings and recommendations were outlined. Recommendations were supported by a detailed action plan. Although, it was noted that actions were not assigned due dates.

Serious Event Report – Testing of the BCP

A report is in place for a test completed for the Communications Function in March 2026. Review of the report confirmed that the methodology and findings were outlined along with an action plan. Further review noted that the report was signed off by the Head of Comms, Engagement and Public Affairs.

Another example of a test scenario completed was provided for the Hearings Team and the findings were accepted in July 2025. Review of the report confirmed that an assurance rating was reported and recommendations were raised. The report was completed by the CISRO and signed off by the Operational Manager - Hearings. Further review of the report noted that methodology and findings were outlined and recommendations were recorded in an action plan.

Summary of Actions for Management

01

SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

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

Ref	Action	Priority	Responsible Owner	Date
1	Processes relating to scenario testing, post incident reviews and escalation and de-escalation of plans will be documented in the Business Continuity Strategy.	Medium	Chief Information Security & Risk Officer	31/07/2026
2	All reviews of the BCP will be documented with evidence of approval by appropriate stakeholders. The next review date will also be recorded in the Plan.	Low	Information Governance & Risk Lead	31/03/2027
3	Training will be provided to staff on a periodic basis in relation to the business continuity arrangements and a record of attendance will be maintained. Any learning identified from incidents and testing of incidents will be incorporated into the cyclical training programme. *Management response:* *Training relating to BCM / DR for general employees will be via the Corporate Induction process and the annual Information Security & Compliance training provided.*	Medium	Information Governance & Risk Lead	29/01/2027
4	Agree a three-year test programme for the business continuity plan. Business areas will be risk assessed and this will be used to inform the timings of testing for each business area.	Medium	Information Governance & Risk Lead	31/03/2027
5	The incident log will be updated to categorise incidents by type.	Low	Chief Information Security & Risk Officer	31/07/2026
6	At agreed intervals, the Information Security and Compliance Group and / or the Information and Technology Governance Board will provide assurance to the Senior Leadership Team (SLT) or Executive Leadership Team (ELT) on business continuity arrangements. This will include the progress made to implement recommendations and actions as well as learning identified from business continuity incidents and tests which have been conducted. *Management response:* *Although a Serious Event Report may be produced for some serious incidents, all learning will be captured in the Improvement Log.*	Medium	Information Governance & Risk Lead	31/03/2027

* Refer to Appendix B for more detail

Detailed Findings and Actions

02

DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all audit testing undertaken.

Area: Business Continuity Plan (BCP)				
Control	There is a Business Continuity Plan (BCP) in place which outlines the business continuity arrangements for each business function. Each action plan outlines the triggers, associated actions and responsible owners. The Plan is reviewed annually and individual plans for each service are reviewed every six months.	**Assessment:** **Design** ✓ **Compliance** ×		
Findings / Implications	**BCP** Review of the BCP dated 5 February 2026 confirmed that for each business function, the Plan outlined the triggers, actions, responsible owners and supporting information for disruption scenarios. This covered the following functions: Governance, Human Resources, Partners, Education, Finance, Fitness to Practise (Tribunal Service) IT Continuity, Office Services and Facilities, Policy and Standards and Registration. Further review noted that the organisation has a dedicated disaster recovery site (Daisy) if there is a London wide emergency, and processes in relation to this are outlined in the BCP. To support this, there is a document entitled 'Department BCM Scenarios' which lists various scenarios for each department which could occur in the event of a business continuity incident. However, review noted that the Plan does not clearly specify the processes and requirements for regular formalised scenario testing, post-incident or post-exercise reviews. Furthermore, the Plan does not outline the escalation procedures if a business continuity incident arises. These processes should be outlined in the Business Continuity Strategy which is already in place and has been adopted. There is a risk that staff are unaware of key processes relating the business continuity. In turn, this could lead to delayed or uncoordinated responses to incidents or inefficient outcomes and learning from tests and incidents.			
Management Action 1	Processes relating to scenario testing, post incident reviews and escalation and de-escalation of plans will be documented in the Business Continuity Strategy.	**Responsible Owner:** Chief Information Security & Risk Officer	**Date:** 31/07/2026	**Priority:** Medium
Findings / Implications	**Review of the BCP** The BCP was dated February 2026 and therefore it can be inferred that the plan was last reviewed this year. However, it was not clear how often the Plan is reviewed. There is a risk that the BCP may become outdated or ineffective, as may not reflect current business operations, risks, or recovery requirements due to the absence of a defined and evidenced review process.			
Management Action 2	All reviews of the BCP will be documented with evidence of approval by appropriate stakeholders. The next review date will also be recorded in the Plan.	**Responsible Owner:**	**Date:** 31/03/2027	**Priority:** Low

		Information Governance & Risk Lead		

Area: Roles and Responsibilities				
Control	Each action outlined in response to a disruption scenario has been assigned a responsible owner. This is outlined in the BCP.		**Assessment:**	
			Design	✓
			Compliance	×
Findings / Implications	For each business function, the Plan lists the responsible owner for each potential business continuity disruption. However, review noted that the roles and responsibilities and processes for escalating and de-escalating plans was not clearly outlined. There is a risk that the HCPC may experience delayed responses to business disruptions due to the absence of clearly documented roles, responsibilities and escalation and de-escalation processes. **Refer to management action 1.**			

Area: Training				
Missing Control	Currently, there is no training programme or equivalent in place for staff in relation to the BCP.		**Assessment:**	
			Design	×
			Compliance	×
Findings / Implications	The Strategy states that the Crisis Response Team and the Service Teams should be trained on an annual basis with respect to the BCP. However, discussions with management informed that there is no formal training programme in place for staff. Management informed that currently training and learning is provided through business continuity tests and the subsequent learnings shared with business area owners, and information provided through ad-hoc workshops. A lack of formal training increases the risk of ineffective incident response and disruption to critical services.			
Management Action 3	Training will be provided to staff on a periodic basis in relation to the business continuity arrangements and a record of attendance will be maintained. Any learning identified from incidents and testing of incidents will be incorporated into the cyclical CBT based training programme.	**Responsible Owner:** Information Governance & Risk Lead	**Date:** 29/01/2027	**Priority:** Medium
Management Response	Training relating to BCM / DR for general employees will be via the Corporate Induction process and the annual Information Security & Compliance training provided.			

Area: Testing of the Business Continuity Plans				
Control	The Chief Information Security and Risk Officer (CISRO) conducts two business continuity tests each year as part of a three year cycle to cover all business areas and relevant business continuity risks. A report is		**Assessment:**	
			Design	✓

Area: Testing of the Business Continuity Plans				
	completed following a test of the business continuity plan. The report is presented to the head of the business area and includes the outcomes from the test, learning and actions.		**Compliance**	×
Findings / Implications	Management informed that tests are completed on a three year cycle and the CISRO is responsible for conducting tests of the BCP with support from the head of the department. A planning phase is undertaken with heads of departments to create scenarios for testing which are relevant to the HCPC and the department. However, there was no evidence of a testing plan or equivalent to confirm that all business areas are tested over this period. Similarly, it was not clear whether testing of business areas is risk assessed to identify which tests should be prioritised based on the associated risks. A lack of a risk-based testing plan increases the risk that key business areas may not be tested and subsequently updated, leading to an ineffective business continuity response.			
Management Action 4	Agree a three-year test programme for the business continuity plan. Business areas will be risk assessed and these will be used to inform the timings of testing for each business area.	**Responsible Owner:** Information Governance & Risk Lead	**Date:** 31/03/2027	**Priority:** Medium

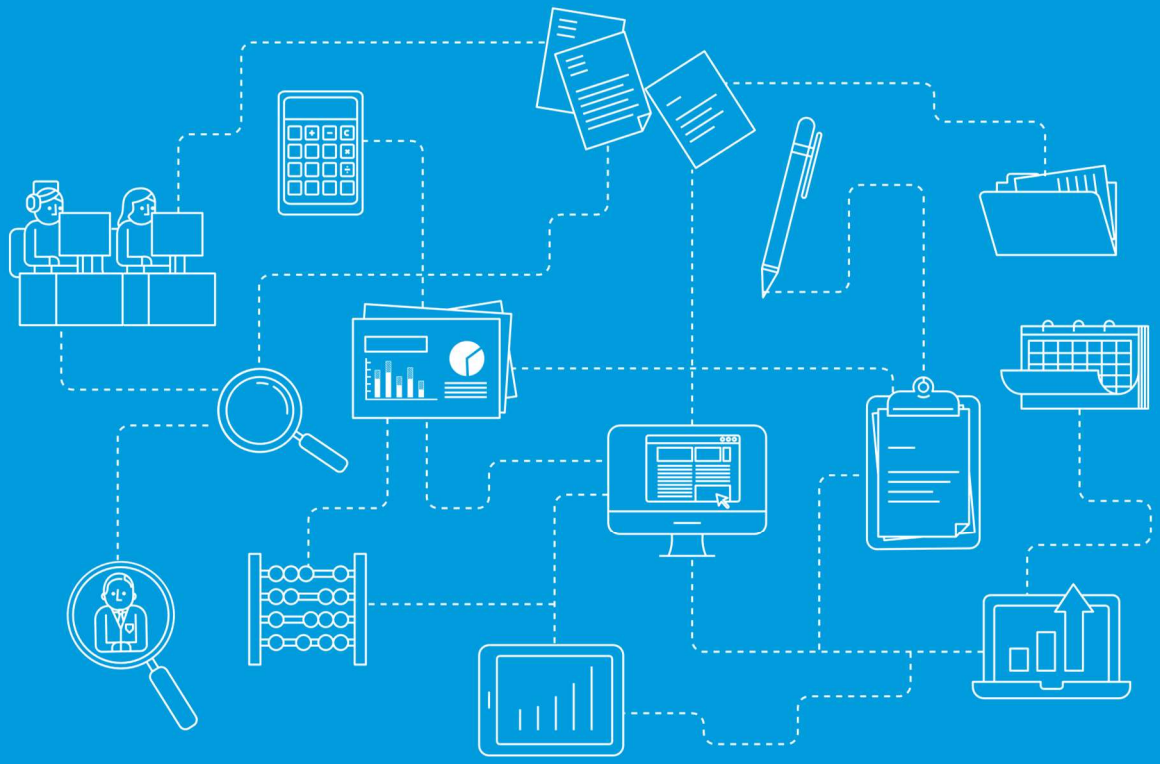
Area: Process to detect and manage business continuity incidents				
Control	Heads of Departments are responsible for identifying and raising an incident with the CISRO. A Serious Event Report (SER) is completed and the event is investigated by the CISRO. Findings and actions are documented in the SER which is shared with the Head of Department. The CISRO maintains a spreadsheet which lists all incidents that have been reported.		**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	An improvement log is maintained by the CISRO which lists all incidents that have occurred. This was reviewed during a walkthrough at the time of audit due to the confidential nature of the information contained in the document. The log included (but was not limited to) key details relating to the incident and audit dates, description of findings, type, raised by, root cause, responsible owners, action dates. However, it was difficult to identify which incidents related to business continuity as the incidents were not categorised by type and therefore, we were unable to confirm how many business continuity incidents had occurred at the HCPC in order to select an adequate sample for testing. Unclear categorising of incidents may result in ineffective oversight and management of business continuity incidents, increasing the risk of prolonged disruptions.			
Management Action 5	The improvement log will be updated to categorise incidents by type.	**Responsible Owner:** Chief Information Security & Risk Officer	**Date:** 31/07/2026	**Priority:** Low

Area: Post incident review process				
Control	After each test or incident, learning is captured in the Improvement Log. Learning is shared where required and used to update the BCP.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	Two test reports and one Serious Event Report were reviewed during our audit. Review of the reports noted that whilst recommendations had been raised and management responses provided, there were instances where actions did not have a clear due date. Furthermore, it was not clear how progress of the actions is monitored to ensure that learning is embedded. It was also noted that there was no evidence provided to confirm that learning was triangulated across the organisation and presented to the Executive Leadership Team or Audit and Risk Assurance Committee. Where learning is identified and not triangulated across the organisation, there is a risk that learning identified from business continuity tests or incidents is not effectively embedded in the organisation, which in turn could reduce resilience to future incidents.			
Management Action 6	At agreed intervals, the Information Security and Compliance Group and / or the Information and Technology Governance Board will provide assurance to the Senior Leadership Team (SLT) or Executive Leadership Team (ELT) on business continuity arrangements. This will include the progress made to implement recommendations and actions as well as learning identified from business continuity incidents and tests which have been conducted.	**Responsible Owner:** Information Governance & Risk Lead	**Date:** 31/03/2027	**Priority:** Medium
Management Response	Although a Serious Event Report may be produced for some serious incidents, all learning will be captured in the Improvement Log.			

Area: Missing Control – Oversight for business continuity arrangements				
Missing Control	Currently there is no governance group or committee that has oversight of business continuity arrangements. As a result, there are no clear reporting lines for business continuity.		**Assessment:** **Design** × **Compliance** ×	
Findings / Implications	Discussion with management informed that there is currently no governance group or committee that has oversight of business continuity arrangements. On an ad-hoc basis or where required, serious incident reports may be presented to the Executive Leadership Team (ELT) for discussion, however this is not on a consistent basis. This could lead to a risk of unclear ownership, inadequate oversight and missed opportunities to share learning from incidents. **Refer to management action 6.**			

Appendices

03



APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings
Low There is scope for enhancing control or improving efficiency.
Medium Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Risk	Control design not effective*	Non-compliance with controls*	Agreed actions		
			Low	Medium	High
There may be extensive disruption to both service delivery and the invigilation of the online registration assessment, resulting in significant delays, cancellations, and concerns around the integrity of the process.	2 / (13)	5 / (13)	2 (33%)	4 (67%)	0 (0%)
Total			**2**	**4**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: INTERNAL AUDIT ASSIGNMENT OPINIONS

Minimal Assurance

Taking account of the issues identified, the board cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Urgent action is needed to strengthen the control framework to manage the identified risk(s).

Reasonable Assurance

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

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

Partial Assurance

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

Action is needed to strengthen the control framework to manage the identified risk(s).

Substantial Assurance

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

APPENDIX C: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following area and risk:

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
An audit on Incident Management and Business Continuity will assess the robustness of plans in place, ensuring they cover critical functions, the testing of these plans, key roles and responsibilities and the assurance mechanisms in place, that in the event an incident arises, the organisation is ready to deploy the plans.	**Strategic Risk 5.a** - The resources we require to achieve our strategy are not in place or are not sustainable.	Strategic risk register
	There may be extensive disruption to both service delivery and the invigilation of the online registration assessment, resulting in significant delays, cancellations, and concerns around the integrity of the process.	Business Risk

When planning the audit, the following were agreed:

Areas for consideration:

- Business Continuity policies and procedures including the requirements in relation to scenario testing, reporting, responsibilities and how national guidance has been incorporated.
- Whether Business Continuity Plans cover critical business areas and dependencies and includes business impact assessments (BIA), risk assessments and outlines recovery priorities.
- Whether the Business Continuity Plans appropriately detail the roles and responsibilities of staff in the event of a disaster/disruption. This includes responsibility for escalating and de-escalating the plan.
- Training in relation to the execution of the Business Continuity Plans (for instance, carrying out a walkthrough of all steps with key staff) is provided to staff.
- Testing of the Business Continuity Plans is undertaken to ensure that key systems can be effectively recovered, shortcomings are addressed, and the plan remains relevant.
- There is a process to detect and manage business continuity incidents. As part of this, we will consider the processes for assessing and triaging incidents and whether records of incidents are maintained.
- There is a post incident review process in place, which includes updating response plans after every incident and providing feedback to the wider organisation.

- Ownership for business continuity arrangements and any dedicated forums for which business continuity is reported, and review and approval of the Business Continuity Plan is undertaken.

Limitations to the scope of the audit assignment:

- We will not confirm the effectiveness of the training provided, only whether the organisation has measures in place to confirm effectiveness of training provided. We will also not confirm the accuracy of the data reported.
- Our audit will exclude IT recovery processes and backup arrangements but will cover how the business responds if there an IT issue.
- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of incident management and business continuity.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- We will not confirm whether all incidents have been identified by the organisation and whether incidents have been correctly classified in terms of severity.
- We will not confirm the effectiveness of the training provided, only whether the organisation has measures in place to confirm effectiveness of training provided. We will also not confirm the accuracy of the data reported.
- We will not provide any guarantees that business continuity arrangements will be effective, in the event of an incident/disaster, only that robust structures and systems are in place to support this.
- Testing will be undertaken on a sample basis only from April 2025.

Our work will not provide an absolute assurance that material errors, loss or fraud do not exist.

Please note that the full scope of the audit can only be completed within the audit budget if all the requested information is made available at the start of the audit and the necessary key staff are available to assist the audit process. Delays in meeting our information requirements may lead to delays in any proposed timetable, which in turn may cause us to incur additional costs; we reserve the right to raise a supplementary invoice for any such additional fees. We will notify you as soon as it is apparent that there are delays with meeting our information requirements and any consequent changes to the timetable.

To minimise the risk of data loss and to ensure data security of the information provided, we remind you that we only require the specific information requested. In instances where excess information is provided, this will be deleted, and the client sponsor will be informed.

Debrief held	8 May 2026	**Internal audit Contacts**	Nick Atkinson – Head of Internal Audit Sarah Howe – Associate Director Clara Agyekumhene – Managing Consultant Faiz Jalaludin – Senior Consultant Elizabeth Casi – Consultant
Draft report issued	21 May 2026		
Responses received	10 June, 25 June and 6 July 2026		
Final report issued	6 July 2026	**Client sponsor**	Claire Amor – Executive Director of Corporate Affairs
		Distribution	Claire Amor – Executive Director of Corporate Affairs Roy Dunn – Chief Information Security and Risk Officer Anna Raftery – Head of Assurance and Compliance Nicole Jones – Improvement and Compliance Specialist

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com.

FOR FURTHER INFORMATION CONTACT

Nick Atkinson, Head of Internal Audit

Email: Nick.Atkinson@rsmuk.com
Telephone: +44 (0) 20 3201 8028

Sarah Howe, Associate Director

Email: Sarah.Howe@rsmuk.com
Telephone: +44 (0) 203 201 8773

Clara Agyekumhene, Managing Consultant

Email: Clara.Agyekumhene@rsmuk.com
Telephone: 020 3201 8797

rsmuk.com