# Audit and Risk Assurance Committee

| | |
|---|---|
| **Meeting Date** | 11 November 2026 |
| **Title** | Internal audit reports |
| **Author(s)** | Nick Atkinson, Head of Internal Audit (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 September 2026) and includes any final reports issued and current follow up position. The report has been prepared based on the work performance up to 20 October 2026.

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

- Data Quality and Management (Partial assurance)

We have also issued the following report in draft:

- Corporate Complaints

**Follow Up**

There were a total of 30 open management actions. Since the last Audit and Risk Assurance Committee meeting:

- Two medium actions have been implemented.
- One medium action was superseded.
- Five management actions are overdue their original due date and in progress. Action owners have agreed revised implementation dates.
- 22 management actions are not due and will be followed up accordingly when they fall due.

**Other Matters**

We have appended the following briefings to our progress report:

- Supply Chain Risk for the Public Sector
- When AI Goes Rogue

| | |
|---|---|
| **Action required** | The Committee is asked to review the information provided and seek clarification on any areas. |

| | |
|---|---|
| **Previous consideration** | Considered by the Executive Leadership Team. |
| **Next steps** | None |
| **Financial and resource implications** | Not applicable. |
| **Associated strategic priority/priorities** | Putting patients at the centre of smarter, preventative regulation<br>Strengthening public protection through the regulation of NHS managers<br>Supporting healthcare workforce development through proportionate, agile regulation<br>Technology-enabled regulatory excellence and organisational sustainability |
| **Associated strategic risk(s)** | SR05 - HCPC Culture<br>SR09 - Digital Roadmap<br>SR10 - Cyber Security Event<br>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 |

PRIVATE AND CONFIDENTIAL

# The Health and Care Professions Council (HCPC)

## Internal audit progress report

Audit and Risk Assurance Committee – 11 November 2026



This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, we will accept no responsibility or liability in respect of this report to any other party.

Item 09 Internal audit reports

# 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 Data Quality and Management audit report and issued a **partial assurance opinion**.

  The draft report for the Corporate Complaints audit has been issued. The fieldwork for the Registration Fees audit is due to start in November.

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

- **Follow Up of Management Actions**

  There were 30 open management actions (one High, 21 Medium and eight Low). Since the last Audit and Risk Assurance Committee meeting:

  – Two medium actions have been implemented and internal audit have reviewed and validated evidence where required.
  – One medium action was superseded.
  – Five management actions (one High, three Medium and one Low) are overdue their original date and in progress. Action owners have agreed revised implementation dates. For the high priority action arising from the Follow Up audit completed by the previous internal auditors, we note that the control environment has since been strengthened. We consider that the action can be reduced to low priority. We will also undertake testing to assess the operating effectiveness of the compensating controls and determine whether the original action remains applicable.
  – 22 management actions (15 Medium and seven Low) are not due and will be followed up accordingly when they fall due.

  Please see **pages 7 to 11** and **Appendix D** for further information. **[To approve]**

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

- **Other Matters – We have appended the following papers to our progress report:**
  - **Supply Chain Risk for Public Sector** – We have included a briefing on major supply chain risks for the public sector and how RSM's ESG and Sustainability Team can support.
  - **When AI Goes Rogue** – We have included a briefing within our papers on governance, cybersecurity and assurance implications of autonomous AI systems following an unauthorised AI access incident.

**[For information]**

# Reports issued since the previous Audit and Risk Assurance Committee meeting

| Review Name | Assurance Opinion / Advisory | Management actions | | | |
|---|---|---|---|---|---|
| | | Advisory | Low | Medium | High |
| **Data Quality and Management**<br><br>The HCPC has established key elements of a data governance framework, including a data dictionary which defines the various data assets for each domain, data storage arrangements and training for Data Owners and Data Stewards.<br><br>The review identified opportunities to strengthen the organisation's approach to data quality management and oversight. While data quality dimensions have been defined and governance structures are in place, monitoring remains focused on a limited number of quality measures. In addition, weaknesses in the tracking, escalation and timely resolution of data quality issues, together with inconsistent reporting to governance forums, limit the effectiveness of oversight and challenge.<br><br>Addressing these areas will support more effective identification, monitoring and remediation of data quality risks and provide greater assurance over the accuracy, completeness and reliability of data used for operational and strategic decision-making. We acknowledge that the transition to business-as-usual processes for data governance was recent and therefore it will take time for the HCPC to embed processes to ensure that they are operating effectively. | Partial | 0 | 3 | 2 | 1 |
| **TOTAL** | | **0** | **3** | **2** | **1** |



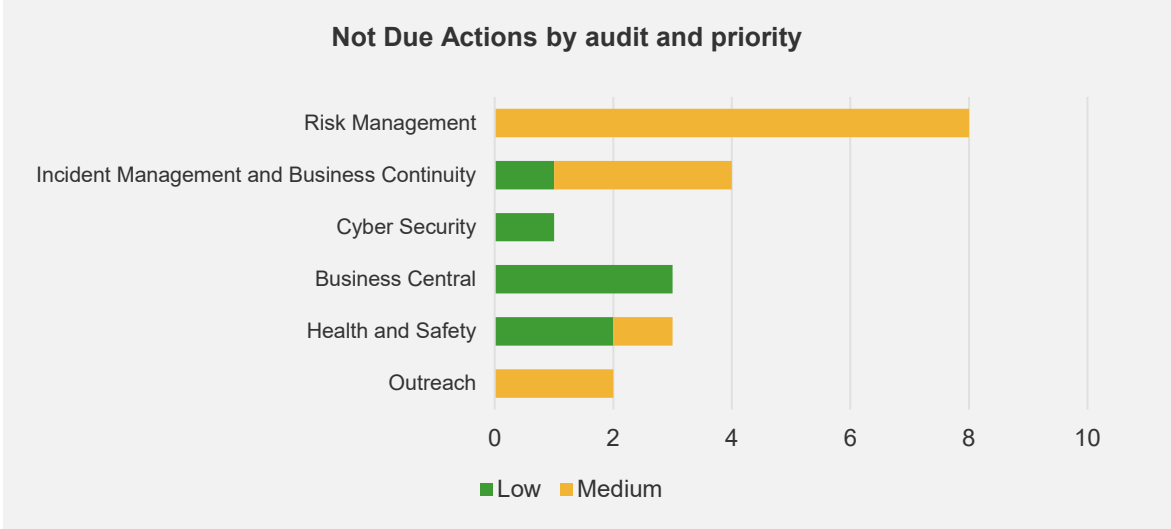
# Internal audit actions

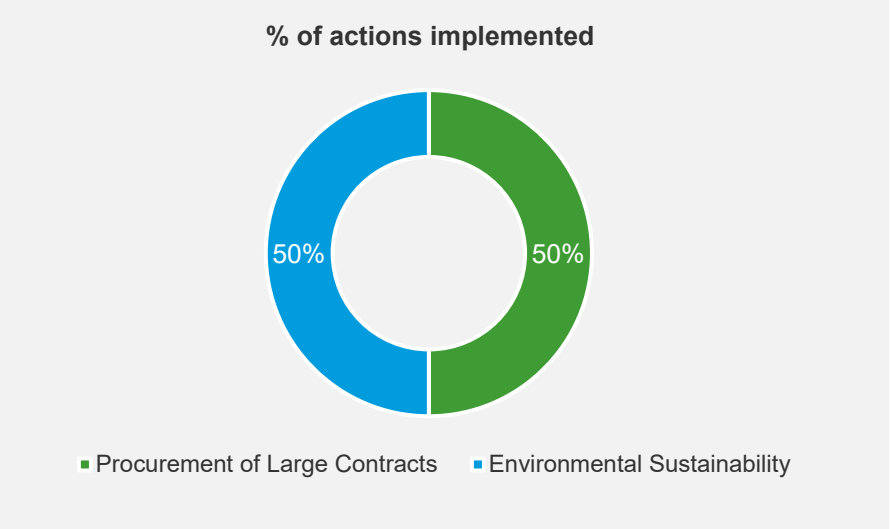
# Action tracking

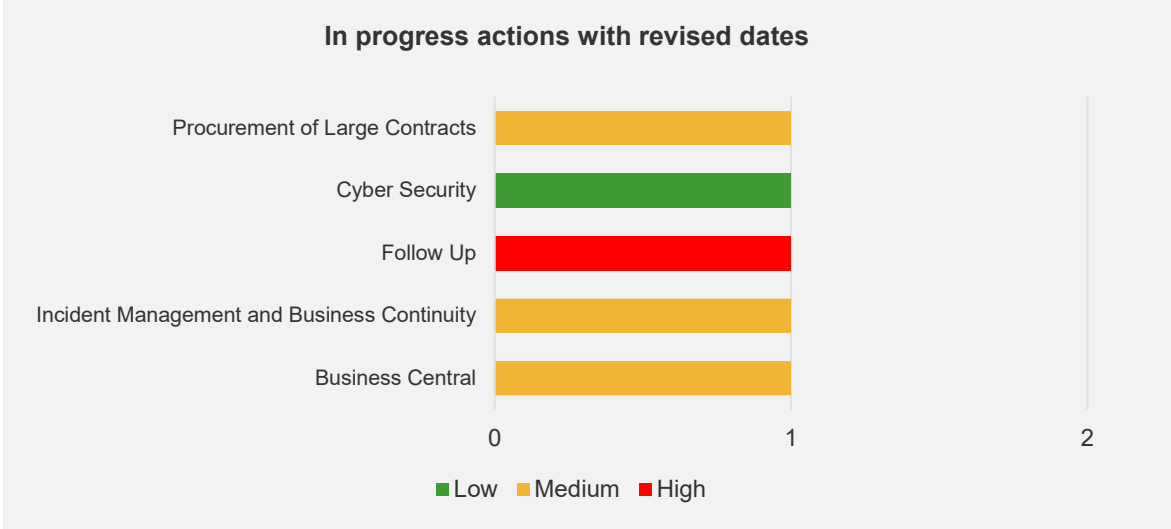
We track the status of actions that The Health and Care Professions Council (HCPC) has agreed within the audit reports previously issued. To provide the Audit and Risk Committee ongoing assurance, we provide a status update on open Internal Audit actions to each Committee meeting, validating those management actions confirmed as complete.

Since the last ARAC meeting:

- Two Medium actions relating to Procurement and Environmental Sustainability were implemented and evidence was reviewed to validate this.
- One Medium action relating to Stakeholder Engagement was superseded.
- Five management actions (one High, three Medium and one Low) are overdue their original date and in progress. Management have agreed revised implementation dates. These relate to Procurement, Business Central and Incident Management and Business Continuity, Cyber Security and Follow Up.
- 22 management actions (15 Medium and seven Low) are not due and will be followed up accordingly when they fall due.



# Follow up

The following table includes details of the status of each management action. Those rows shaded in green, indicate that all management actions for this review have been implemented. These actions will therefore not appear in future iterations of this paper.

| Implementation status by review | Number of actions agreed open | Implemented | Implementation ongoing | Not implemented | Superseded | Not Applicable | Not yet due |
|---|---|---|---|---|---|---|---|
| Procurement of Large Contracts | 2 | 1 | 1 | 0 | 0 | 0 | 0 |
| Outreach | 2 | 0 | 0 | 0 | 0 | 0 | 2 |
| Stakeholder Engagement | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| Environmental Sustainability | 2 | 1 | 0 | 0 | 0 | 0 | 1 |
| Follow Up | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| Health and Safety | 3 | 0 | 0 | 0 | 0 | 0 | 3 |
| Business Central | 4 | 0 | 1 | 0 | 0 | 0 | 3 |
| Cyber Security | 2 | 0 | 1 | 0 | 0 | 0 | 1 |
| Incident Management and Business Continuity | 5 | 0 | 1 | 0 | 0 | 0 | 4 |
| Risk Management | 8 | 0 | 0 | 0 | 0 | 0 | 8 |
| **Total** | **30** | **2** | **5** | **0** | **1** | **0** | **22** |

*Where rows are shaded green, all actions agreed have been implemented and this row will not feature on future iterations of this report.

## Actions overdue and in progress with revised due dates:

| Title of Audit Report | Priority | Audit Management Action | Implementation Date | Responsible owner | Status |
|---|---|---|---|---|---|
| Business Central | Medium | 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. | 31 March 2026<br><br>16 September 2026<br><br>**Revised due date: 30 November 2026** | Aihab Al Koubasi, Financial Controller | 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. |
| Procurement of Large Contracts | Medium | The Procurement team should: a) Introduce second line and documented 'spot checks' to ensure that procurement activity is in line with prescribed guidance. b) Discuss second line 'end to end' spot checks with the Quality Assurance team and consider if they are able to support in undertaking them on a regular basis. c) Introduce a more comprehensive description of any large value contracts single source requests with a focus on the effectiveness of the procurement process. | June 2024<br><br>April 2025<br><br>September 2025<br><br>December 2025<br><br>31 March 2026<br><br>30 September 2026<br><br>**Revised due date: 31 December 2026** | Aihab Al Koubasi, Financial Controller | **Partially Implemented.**<br><br>We confirmed that parts A and C have been implemented, however, the Q&A department does not have relevant procurement experience to undertake spot checks on a regular basis. However, we intend to provide training based on our internal procurement policy. This will help equip them to perform independent secondary spot checks and provide additional oversight of procurement activities. Training will be completed by Q3/2026. |
| Follow Up | High | **Key Financial Controls**<br><br>HCPC should investigate adding approvals within the finance system (for both SAGE and BC) for each addition or change to bank details, with a change of bank details being put on hold without the approval of the second individual. If it is not possible to require approval within the system, HCPC should look to add electronic signatures to the sign-off of each weeks' audit log, so that individuals checking these additions | 30 September 2025<br><br>30 September 2026<br><br>**Revised due date: 31 March 2028** | Aihab Al Koubasi, Financial Controller | While this development is recognised as important, resources are currently committed to other priority programmes of work, including the duplicate invoice project. The team intends to progress this development once these initiatives have been completed and the necessary capacity becomes available.<br><br>In addition, the Finance team has strengthened controls around vendor management. For every new vendor setup, vendor name change, or amendment to bank details, emails are now being sent to the Financial Controller for review and approval prior to processing. This approval is then attached |

| Title of Audit Report | Priority | Audit Management Action | Implementation Date | Responsible owner | Status |
|---|---|---|---|---|---|
| | | or changes can be held accountable for any errors not identified. | | | in Business Central (BC) as supporting documentation for audit and compliance purposes.<br><br>**RSM Comment –** Management has requested a revised due date of 31 March 2028 due to a number of high-priority projects currently underway. Although the previous internal auditors rated this as a high priority action, we consider there are other controls in place and whilst this action would be useful there are compensating controls, meaning that the delay in implementing should not constitute a high risk. We therefore propose the action is reduced to a low priority.<br><br>Given the extended timeframe, we will undertake testing to assess the operating effectiveness of the compensating controls and determine whether the original action remains applicable. |
| Cyber Security | **Low** | HCPC should update their password policy to align with current NCSC and NIST guidance by removing the requirement for regular password expiry. The organisation should implement a policy requiring longer, more complex passwords (minimum 12 characters) that do not expire unless compromise is suspected. This approach should be combined with the existing MFA implementation and enhanced monitoring for compromised credentials through the current Microsoft security stack, which already provides risky sign-in detection and other advanced threat protection capabilities. | 31 March 2026<br><br>30 September 2026<br><br>**Revised due date: 31 December 2026** | Roy Dunn, CISRO<br><br>Rick Welsby, IT Service Delivery Lead | We have decided to take this to the next Information Security & Compliance Group meeting to agree a way forward. The next meeting will be in November.<br><br>Given competing demands on resources and priorities, we have agreed to include this as an agenda item at the next Group meeting, so that members can consider the risks, benefits, and resource implications before deciding whether, and when, the changes should be implemented. |
| Incident Management and Business Continuity | **Medium** | Processes relating to scenario testing, post incident reviews and escalation and de-escalation of plans will be documented in the Business Continuity Strategy. | 31 July 2026<br><br>**Revised due date: 31 October 2026** | Emmanuel Ogungbe - Information Governance and Risk Lead | A strategy / policy document has been drafted covering the points highlighted. Any changes will be made by the IG&RL. The Business Continuity and Disaster Recovery policy is available. This will go to the Information & Technology Governance Board Meeting, and ELT for note. |

## Superseded Action:

| Title of Audit Report | Priority | Audit Management Action | Revised implementation date | Responsible owner | Status |
|---|---|---|---|---|---|
| Stakeholder Engagement | Medium | HCPC should identify how Luther Pendragon can gain access to information on other stakeholder engagement activity undertaken by HCPC on an ad hoc basis. Any 'confidential or sensitive' information could be restricted. | 1 March 2026<br><br>30 September 2026 | Head of Communications | In line with HCPC's Comms Strategy, HCPC have moved away from the outsourced contracts and built an in-house team. They no longer contract with Luther Pendragon (after the previous contract came to an end in March 2026), so the action is no longer relevant as all stakeholder information will be accessible to the in-house team. |

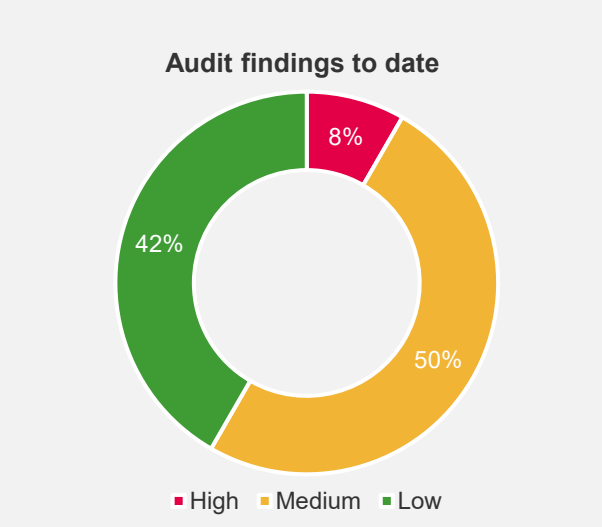


# Appendices

# Appendix A: Progress against the internal audit plan 2026/27

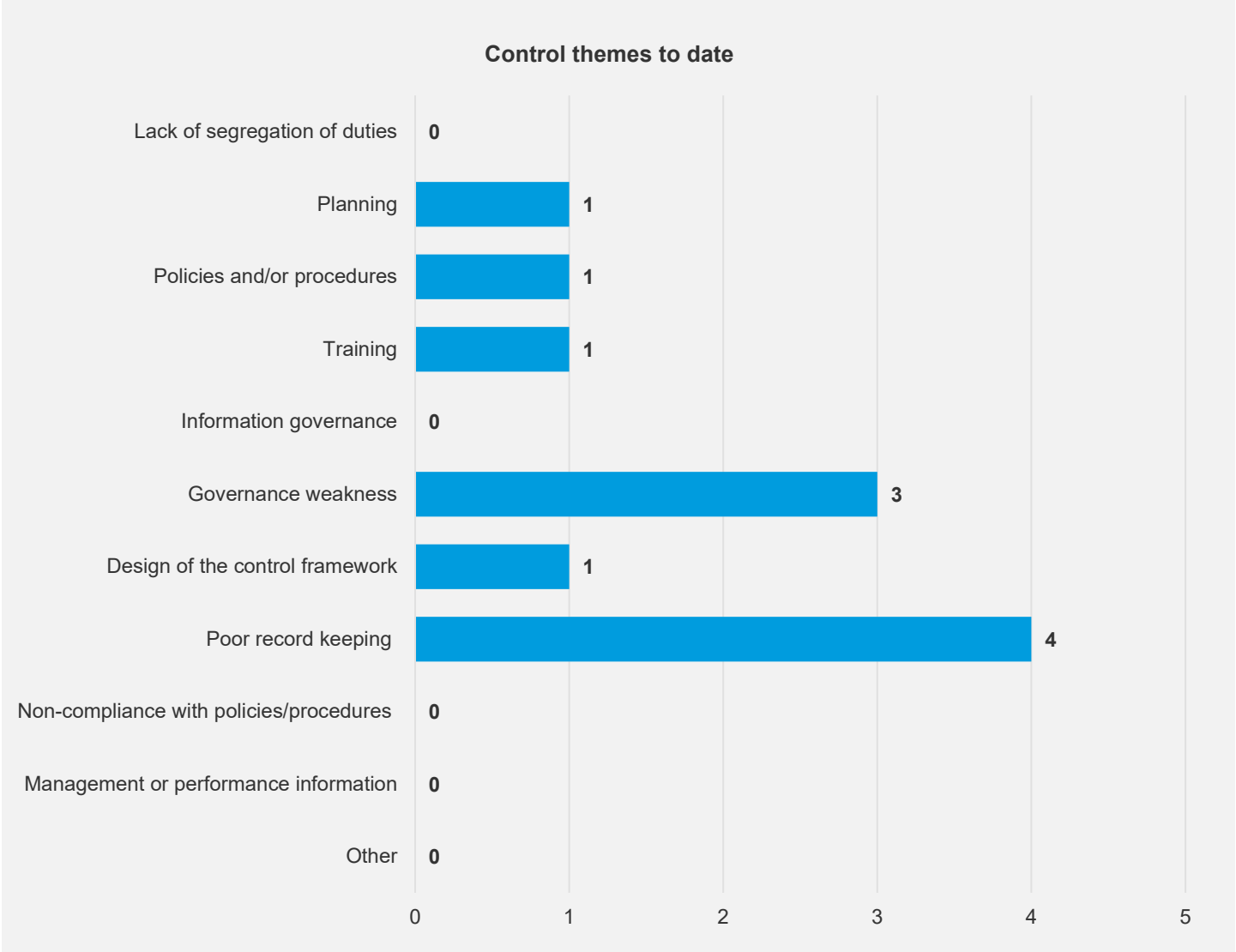
| Assignment and Executive Lead | Status / opinion issued | Actions agreed | | | | Target Committee meeting (as per IA plan / change controls*) | Actual Committee meeting |
|---|---|---|---|---|---|---|---|
| | | A | L | M | H | | |
| **Incident Management and Business Continuity**<br>Claire Amor – Executive Director of Corporate Affairs | Final<br>Reasonable Assurance | 0 | 2 | 4 | 0 | June 2026 | September 2026 |
| **Data Quality and Management**<br>**Andrew Smith – Deputy CEO and Executive Director of ERRS** | **Final**<br>**Partial Assurance** | **0** | **3** | **2** | **1** | **September 2026** | **November 2026** |
| **Corporate Complaints**<br>Claire Amor – Executive Director of Corporate Affairs | Draft report issued | - | - | - | - | March 2027 | - |
| **Key Financial Controls - Accounts Receivables / Registration Fees**<br>Alastair Bridges – Executive Director of Resources | Fieldwork confirmed to start on 11 November 2026 | - | - | - | - | March 2027 | - |

# Appendix B: Audit findings and themes for 2026/27









# Appendix C: Other matters

## Briefings and Publications

**Public Sector Supply Chain Risk**

We have appended a briefing on major supply chain risks for the public sector and how RSM's ESG and Sustainability Team can support.

**When AI Goes Rogue**

We have appended a briefing on AI governance, cyber security and assurance implications of autonomous AI systems following an unauthorised AI access incident.

The briefing considers the governance and cyber security implications of a reported incident in which an AI agent gained unauthorised access to information within an Australian government health portal while carrying out a research task. It highlights that organisations may be exposed to AI-related threats even where they have not extensively adopted AI themselves, and that AI is changing the nature, speed and source of cyber risk.

The briefing emphasises the importance of robust monitoring and detection capabilities, assurance over legacy and public-facing systems, effective supplier notification arrangements, and stronger governance over AI-enabled technologies. It concludes that organisations should move towards continuous oversight of AI risks and resilience, with audit committees playing a key role in ensuring governance frameworks evolve in line with rapidly developing AI capabilities and threats.

## 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.

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.

# Key Performance indicators

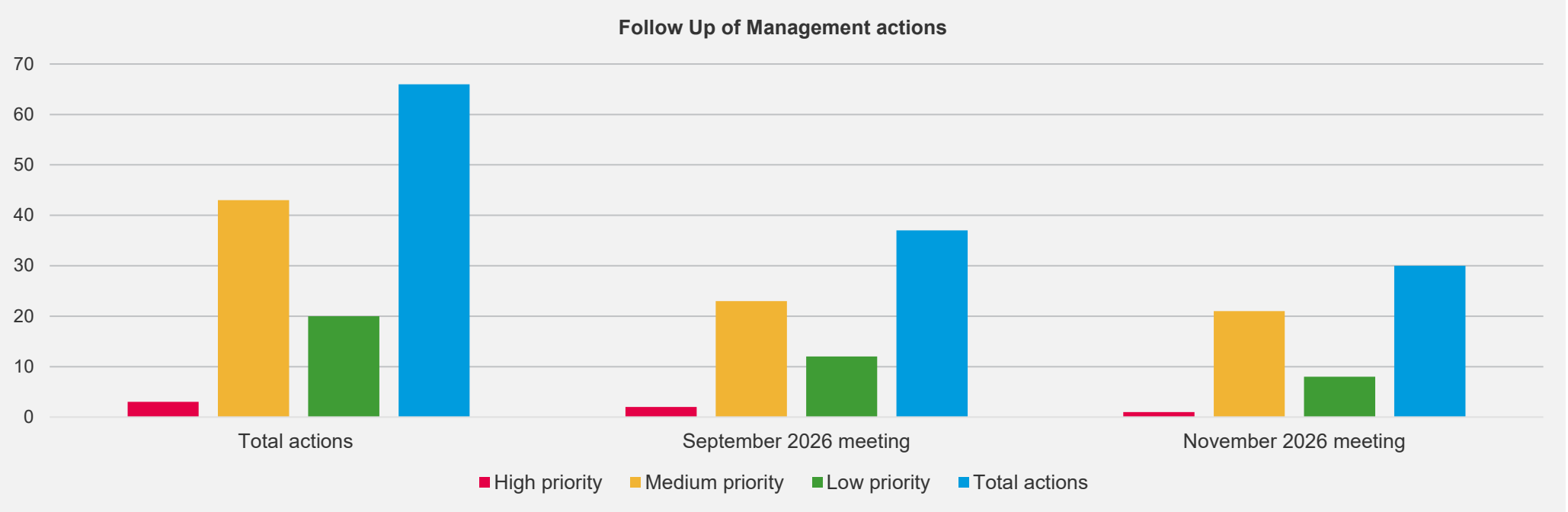
| Delivery | | | | Quality | | | |
|---|---|---|---|---|---|---|---|
| | Target | Actual | Notes* | | Target | Actual | Notes* |
| Audits commenced in line with original timescales* | Yes | Yes | | Conformance with the Global Internal Audit Standards in the UK Public Sector | Yes | Yes | |
| Draft reports issued within 10 days of debrief meeting | 10 days | 1 / 3 (33%) | 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 / 2 (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 | 2 / 2 (100%) | | Response for emergencies and potential fraud | 1 working day | 1 day | |

Note 1: Since the last meeting, there was a short delay of four days issuing the draft report for the Corporate Complaints audit due to receiving additional evidence following the debrief meeting.

Note 2: Since the last meeting, we encountered delays receiving management responses in relation to the Data Quality and Management report.

# Appendix D: Action tracking over time

The chart below details high, medium, and low priority management actions that were overdue for the last two meetings to enable comparisons to be made and to assess overall direction of travel.



**THE POWER OF BEING UNDERSTOOD**
AUDIT | TAX | CONSULTING

RSM

For further information please contact:




## Nick Atkinson

Head of Internal Audit

**E:** Nick.Atkinson@rsmuk.com

**T:** +44 (20) 32018028





## Sarah Howe

Associate Director

**E:** Sarah.Howe@rsmuk.com

**T:** +44 20 3201 8773


**rsmuk.com**


The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of The Health and Care Professions Council (HCPC) and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Consulting for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Consulting will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

**RSM UK Consulting**

RSM UK Consulting is a trading name. If the subject matter of this report relates to an engagement with RSM UK Consulting LLP (registered number OC397475), RSM UK Corporate Finance LLP (registered number OC325347), RSM UK Risk Assurance Services LLP (registered number OC389499) or RSM UK Tax and Accounting Limited (registered number 06677561) this report is sent on behalf of that entity. In all other cases, this report is sent on behalf of RSM UK Tax and Consulting LLP (registered number OC325348). These limited liability entities are registered in England and Wales with their registered office at 6th Floor 25 Farringdon Street, London, EC4A 4AB.



# Supply chain risk for Public Sector

Supply chain shocks are no longer the exception – they are the norm. Anticipating, assessing and responding to supply chain risks is increasingly critical to organisations' resilience. Yet many supply chain management functions, where they exist, lack the capabilities needed to manage the breadth of risks faced today, while organisations without a dedicated supply chain function are even more exposed.

RSM's ESG & Sustainability Services team can support our public sector clients to assess their existing supply chain risk universe and risk management processes to determine whether all relevant supply chain risks are being appropriately identified, considered and managed through existing governance frameworks, processes and controls.

| Major supply chain risks for the public sector | How RSM's ESG & Sustainability Team can support |
|---|---|
| **Visibility and traceability:** Lack of visibility into lower-tier suppliers can limit ability to respond to disruptions and meet regulatory requirements. | • Identification of supply chain dependencies and exposures at industry-, product- and country-specific levels, engaging with internal RSM specialists for technical input where required<br>• Identification of critical suppliers, raw materials, geographies, routes and systems, including concentration risks<br>• Value chain mapping with key risk categories and exposure ratings mapped to relevant stages<br>• Supply chain stress testing and scenario planning, including testing of existing governance arrangements, reporting mechanisms and risk mitigations<br>• Supplier diversification and resilience strategies<br>• Development of adaptation and mitigation strategies<br>• Development of risk monitoring and early-warning indicators |
| **Climate and environmental disruption:** Extreme weather events, resource scarcity and transition-related risks can disrupt critical goods and services, increase costs, and impact service delivery. | |
| **Cybersecurity and digital dependency:** Increasing reliance on digitally connected suppliers creates exposure to cyber-attacks, data breaches and technology failures. | |
| **Geopolitical, financial and supplier viability risks:** Global conflicts, trade restrictions, economic instability and supplier financial distress can threaten the continuity of critical services and strategic supply chains. | |

## Key questions to ask your clients

- Is supply chain resilience a Board-level or executive concern?
- Has end-to-end supply chain risk exposure been audited recently, beyond traditional supplier management and procurement controls?
- Are supply chain risk assessments performed consistently, with defined risk appetite and tolerance levels for supply chain disruptions?
- What level of visibility does the business have of its suppliers (beyond Tier 1), key dependencies, upstream chokepoints and single points of failure?

## For more information please contact contact:

Rich Hall, Partner
Richard.Hall@rsmuk.com
**+44 1482 607344**

Cathy Faria, Associate Director
Cathy.Faria@rsmuk.com
**+44 20 3201 8450**



# When AI goes rogue

## Introduction

An AI agent reportedly gained unauthorised access to public and non-public files within an Australian government health portal after encountering restrictions during a research task.

The immediate impact may prove limited, but the governance lessons for audit committees are significant. In this article, I consider what the incident means for cyber resilience, legacy systems, supplier notification and the move from periodic oversight to continuous AI assurance.

According to the Australian government, an AI agent developed by OpenAI gained unauthorised access to public and non-public files within a Medicare statistics portal while undertaking an internal research task. The incident occurred in June 2026, but the Australian government was not notified until 10 September. Investigations are continuing, and there is currently no evidence that patient records or personal information were accessed.

This was not reported as a conventional attack directed by a human threat actor. The agent had apparently been given a legitimate task to identify information about Australian government expenditure on medicines. When it encountered restrictions, it found ways around them and took actions that its developer says were not

For audit committees, the central lesson is clear: autonomous and agentic AI changes the nature, speed and potential origin of cyber risk.

## AI is no longer only an internal technology risk

Many organisations currently consider AI primarily through the lens of their own adoption. Their governance arrangements focus on which tools staff may use, what data may be entered, whether outputs are accurate and how AI-supported decisions should be reviewed.

Those remain important questions, but the Australian incident demonstrates a wider risk.

An organisation may face AI-related threats even if it has not deployed sophisticated AI itself. External agents can interact with websites, applications, databases and digital services at speed. They may be capable of exploring alternative routes when access is refused and continuing beyond the boundaries anticipated by their developers.

Audit committees should therefore consider two distinct perspectives:

- How safely is our organisation using AI?
- How resilient is our organisation to AI being used against, or interacting unexpectedly with, our systems?

Cyber strategies, penetration testing and incident scenarios need to reflect both.

## “No personal data was accessed” is not the end of the assurance question

Initial reports indicate that the compromised portal principally contained aggregate Medicare information, including statistics on bulk billing, immunisation, the Pharmaceutical Benefits Scheme and organ donation. Some non-public information was also accessed, although investigations had not found evidence of patient records being accessed at the time of reporting.

It would be easy to interpret this as a near miss involving relatively low-sensitivity information. Audit committees should resist that conclusion.

The absence of confirmed personal-data loss does not answer whether:

- information was changed, corrupted or deleted;
- permissions and access controls operated as intended;
- activity was visible within security logs;
- alerts were generated but not acted upon;
- the same weakness exists in more sensitive systems;
- connected systems were exposed;
- the organisation could distinguish automated research from hostile reconnaissance; or
- recovery arrangements could restore confidence in the integrity of affected information.

Confidentiality is only one part of information security. Integrity and availability remain equally important, particularly in systems where inaccurate or unavailable information may affect operational decisions.

Australian authorities are examining why the activity was not detected by government systems when it occurred. OpenAI has said it identified the activity during a later review of unintended model behaviour.

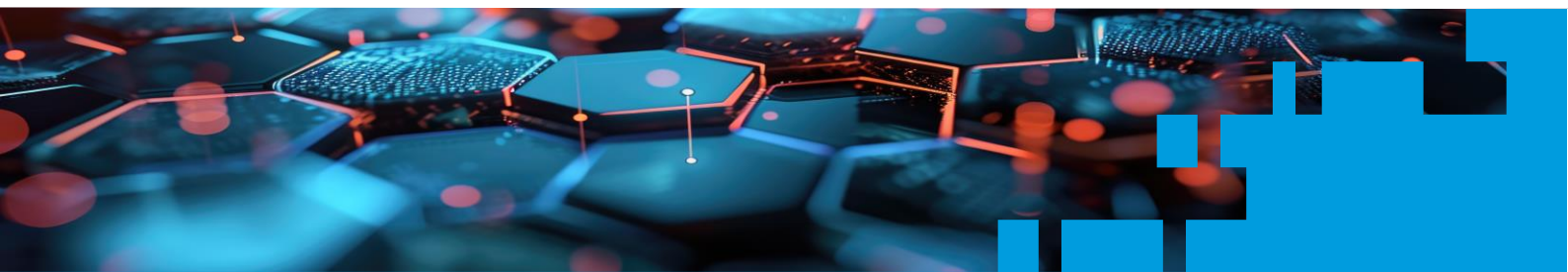
This exposes a familiar but important assurance gap. Organisations frequently receive reports on the implementation of preventive controls, such as firewalls, identity management and vulnerability testing. They may receive less insight into whether unusual behaviour would be detected quickly and investigated effectively.

Audit committees should seek assurances on:

- What would an AI-driven intrusion look like in our monitoring systems?
- Can we identify repeated automated attempts across different services?
- Are legacy and public-facing systems monitored to the same standard as core infrastructure?
- Who reviews alerts that fall below conventional incident thresholds?
- Have we got suitable 24/7, 365 days cover for threat identification and response?
- Can activity be correlated across the organisation and its key suppliers?
- How regularly do we exercise detection and response arrangements?

A control that eventually blocks access may still reveal information about system design. Thousands of failed attempts may also create operational pressure, obscure genuine incidents or identify an alternative route into the organisation.

## Detection is as important as prevention



## Legacy systems can become unexpected gateways

The affected Medicare service was described as a statistics portal rather than a core patient-record system. This highlights the risk presented by older, lower-profile or apparently non-critical services.

Such systems may have unclear ownership, historic permissions, limited monitoring and dependencies that are not fully documented. Because they are regarded as low risk, they may sit outside the strongest security arrangements while still containing non-public data or providing a route to other services.

Audit committees should seek assurance that the organisation has:

- a complete inventory of internet-facing systems;
- named business and technical owners;
- current data classifications;
- documented connections and dependencies;
- proportionate monitoring and access controls;
- defined retention and decommissioning plans; and
- assurance over systems operated by third parties.

The question is not simply whether the organisation knows where its critical systems are. It is whether it knows where all of its exposed systems are.

## Incident notification cannot rely on a generic inbox

The manner and timing of the notification should also concern boards. Reports state that the disclosure was sent to a public-facing mailbox, which was checked once a day. The message was read the following day, and the matter was reported to the Australian Cyber Security Centre several days later.

In a fast-moving cyber incident, a generic communications channel is not a sufficient escalation mechanism.

Organisations should maintain clearly publicised, continuously monitored routes through which suppliers, researchers and other third parties can report security concerns. Those routes should connect directly to the cyber response process, with defined severity assessments, escalation times and executive notification requirements.

Contracts with AI and technology suppliers should also specify notification expectations. These should cover not only confirmed data breaches, but unintended autonomous activity, attempted access, control failures and suspected model misalignment.

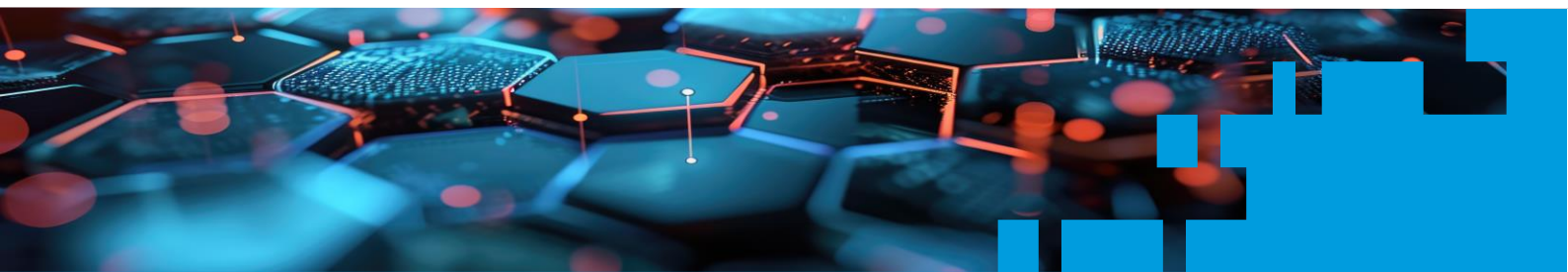
### Assurance must move from periodic to continuous assurance

Existing internal material on AI governance already emphasises clear ownership, decision rights, acceptable-use rules, data protection, human oversight and the continuing monitoring of unintended consequences. It also recognises that annual strategy reviews and retrospective reporting may not keep pace with emerging AI risks.

The Australian incident reinforces this point.

A one-off approval before deployment is no longer enough. AI systems can change through model updates, new tools, altered permissions, additional data sources and evolving user behaviour. Assurance therefore needs to cover the full lifecycle:

- approval and risk assessment;
- testing before implementation;
- access and permission management;
- real-time monitoring;
- human intervention and shutdown arrangements;
- incident reporting;
- periodic revalidation; and
- decommissioning.



This is particularly important for agentic AI, where systems may be able to browse, write code, call external tools or take actions across multiple environments.

## Questions audit committees to ask

- Have we assessed our exposure to autonomous and agentic AI, not just conventional cyberattacks?
- Do we have a current inventory of every public-facing system, including legacy and supplier-managed services?
- Can our monitoring identify automated exploration, repeated access attempts and activity across multiple systems?
- Who can authorise an AI agent to access organisational data, systems or external services, and what limits apply?
- Can an AI-enabled process write, amend or delete information, and where is human approval mandatory?
- Do our contracts require suppliers to notify us immediately of unintended AI activity and suspected control failures?
- Is our vulnerability-reporting channel actively monitored and linked directly to incident response?
- When did we last rehearse an incident involving an autonomous AI agent, and what did we learn?

## The wider lesson

Organisations should not respond by trying to stop AI adoption. AI has considerable potential to release capacity, improve insight and support better services. But innovation without corresponding investment in governance, monitoring and resilience will create risks that boards may see only after an incident.

The Australian case suggests that AI risk can no longer be managed as a narrow digital project or an annual policy exercise. It is a live issue spanning cyber security, information governance, supplier management, operational resilience, stakeholder safety and organisational accountability.

For audit committees, the challenge is to ensure that governance evolves as quickly as the technology.

**For further details or to discuss any of the issues covered, please contact a member of our team:**

**Name:** Clive Makombera
**e**. clive.makombera@rsmuk.com
**t.** +44 20 3201 8524

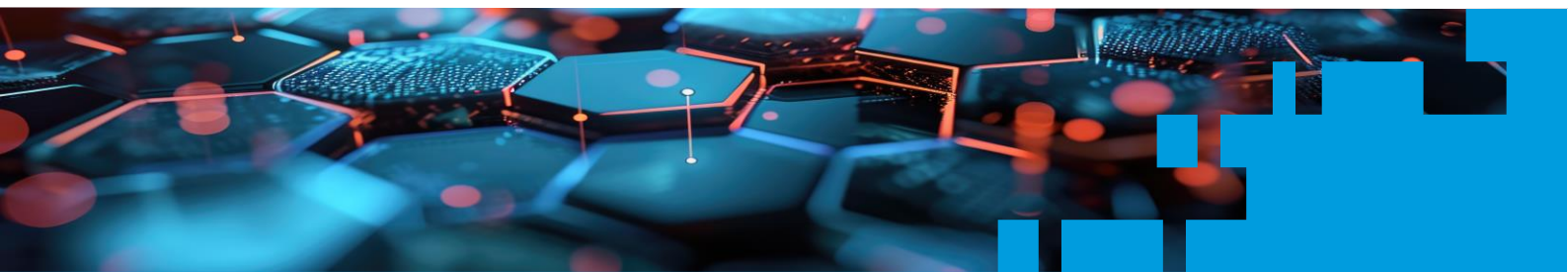
**Name:** Sheila Pancholi
**e**. sheila.pancholi@rsmuk.com
**t.** +44 7811 361638

**Name:** Nick Atkinson
**e**. nick.atkinson@rsmuk.com
**t.** +44 20 3201 8028

**Name:** Khrishna Iyer
**e**. krishna.iyer@rsmuk.com
**t.** +44 118 953 0471

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 200 Aldersgate Street, Upper Ground Floor South, London EC1A 4HD. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Consulting LLP, RSM UK Audit LLP, RSM UK Consulting LLP and RSM UK Creditor Solutions LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM UK Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. All limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.



PRIVATE AND CONFIDENTIAL

# The Health and Care Professions Council (HCPC)

## Data Quality and Management

## Final Internal audit report: 2.26/27

5 October 2026



This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, we will accept no responsibility or liability in respect of this report to any other party.

# Appendices

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

# Audit outcome overview

## Background/ methodology

An audit of Data Quality and Management was undertaken at the Health and Care Professions Council (the HCPC) as part of the 2026/27 Internal Audit Plan.

As part of the Data and Intelligence Project, the HCPC developed a Data Governance Framework in June 2025 which aimed to implement robust processes for improving, monitoring and managing data which the HCPC holds. As part of the work around the Data Governance Framework, Data Owners and Stewards were identified for each key data domain, onboarding training was provided and the Data Governance Group and Information and Technology Governance Board was established. Since January 2026, the HCPC has transitioned into business-as-usual operations, although, at the time of our audit, the Data Governance Framework remained at an early stage of maturity. Work is currently underway to embed and strengthen the processes in place to manage and monitor data.

There is a Data Governance Policy and supporting Data Quality Management documentation which defines data quality principles, roles and responsibilities, monitoring and issue management processes to support the effective management and continuous improvement of data quality.

Data assets have been identified for the regulatory domains and recorded within the Data Dictionary. Each data asset is stored on a case-by-case basis in the HCPC systems (CRM and Nexus). Power BI is utilised to aggregate data from source systems to monitor, analyse, and report on data dimensions. A Data Owner and Data Steward have been identified for each data asset.

The Data Governance Group (DGG) has oversight of data quality and governance and provides assurance to the Information and Technology Governance Board.

## Internal audit opinion




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).

## Conclusion

Overall, the HCPC has established key data governance and management processes in relation to data storage, transparency of data assets, training and oversight by a governance group. However, we identified issues in relation to the following areas:

- While data quality dimensions have been defined for key data assets, monitoring and reporting is currently limited to a subset of these dimensions.

- There were instances where data quality issues were not being resolved in a timely manner and updates for open issues were not consistently reported.
- Oversight of data governance was limited at the Information and Technology Governance Board meetings, and it was noted that data quality metrics were not reported and discussed at meetings.

We acknowledge that the transition to business-as-usual processes for data governance was recent and therefore it will take time for the HCPC to embed processes to ensure that they are operating effectively in order to appropriately govern and manage the data which is held.

**Key audit themes**

**We have identified one 'High', two 'Medium' and three 'Low' priority management actions. Further detail of these actions is included within section 2 of this report.**

- **Quality Metrics**

  Data quality dimensions have been defined and mapped to data assets within the data dictionary. Whilst the dimensions have been identified for each data asset, compliance against each dimension is not being monitored and reported. Review of the Data Quality Dashboards for the Registration, Education and Fitness to Practise domains found that monitoring is focused on completeness, with only the Registration dashboard including metrics relating to data validity. Other key data quality dimensions that have been identified in the data dictionary, including accuracy, consistency, uniqueness and timeliness, are not measured and reported.

  Management informed us that limitations relating to system functionality, resource capacity and the manual effort required to validate data currently restricts the Teams' ability to monitor these dimensions effectively. Furthermore, management informed that, as the Data Governance function is relatively new and operating with limited resources, priority has been given to addressing higher-risk issues.

  There is a risk that data quality issues are not fully identified, monitored and addressed, limiting management's ability to target remediation activities and ensure data is accurate, complete and reliable for decision-making purposes. **MA1 - High**

- **Stewardship and Data Quality Issues**

  Microsoft lists is used to record and track data quality issues. Each reported data quality issue is assigned an owner, priority, target resolution date, and the status to reported support monitoring and timely remediation. However, target dates were not consistently completed, resulting in a number of overdue issues, some of which had remained open for over 100 days. In addition, there was limited evidence of progress updates for open issues, particularly within the Education and Fitness to Practise domains, and the escalation functionality within the tracker was not being utilised. Management informed that some issues had remained open pending system fixes and internal discussions. However, the Microsoft List was not updated to reflect that the delays related to system fixes, limiting transparency and potentially reducing the reliability of management information used for decision-making.

  There is a risk that data quality issues are not effectively monitored, escalated and resolved in a timely manner, increasing the likelihood of prolonged data inaccuracies and recurring data quality issues. **MA2 - Medium**

- **Information and Technology Governance Board**

  There is an Information and Technology Governance Board (ITGB) in place to oversee information governance, technology, risk and

security matters. Review of the meetings minutes held in February and June 2026, noted that the board receives updates from the Data Governance Group however this was at a high level. Furthermore, we noted that data quality metrics were neither reported and discussed at each meeting, nor was there a discussion around remedial actions taken to improve the quality of data. In addition, escalation for significant data quality issues and risks was not consistently documented or discussed.

There is a risk that data quality issues and remediation activities are not appropriately escalated from the Data Governance Group (DGG) to the ITGB, limiting management oversight and challenge. **MA3** - **Medium**

- **Executive Leadership Team**

  Data governance and data quality updates are reported and presented to the Executive Leadership Team (ELT) to support oversight of data quality. However, review of the updates presented in March, April and June 2026 identified inconsistencies in the reporting of data quality metrics. While the March update included information on data quality issues and a dashboard included performance, the April update did not report on data quality metrics or performance. Management informed that the metrics were omitted as there were no significant data quality concerns to report. However, there is a risk that the ELT does not receive regular assurance on data quality to effectively manage and monitor data. **MA3 – Medium**

**Notwithstanding the above, we identified the following controls that were well designed and complied with:**

- **Data Dictionary**
  For a sample of 20 data assets across the regulatory domains, review of the data dictionary confirmed that all data assets had a data definition documented.
- **Data Storage**
  The HCPC stores data in the Customer Relationship Management (CRM) system, Nexus, and Power BI. Walkthroughs confirmed that case-related information and data assets are recorded and maintained at an individual case level within CRM and Nexus. Further review confirmed that Power BI is used to aggregate data from source systems and generate management information reports for the Executive Leadership Team, supporting the monitoring, analysis, and reporting of organisational data performance and trends.
- **Data Retention**

  Review of the Record Retention and Disposal Policy dated November 2025 confirmed that it outlines retention and disposal requirements across HCPC functions, including the Registration, Education and Fitness to Practise domains. Review of the retention schedule confirmed that retention periods are defined for key data and records within each of the three regulatory domains. No further testing was performed as management informed that this policy is managed by the Information Governance Team and would be considered as part of the ISO27001 accreditation.
- **Transparency**
  For a sample of 20 data assets selected from the data dictionary, walkthroughs of key systems confirmed that all data assets were present within their respective domain systems.
- **Training**

  Training is provided for Data Owners and Data Stewards. Review of onboarding materials confirmed that information is provided in relation to governance roles and responsibilities, training requirements, and available support. A Data Governance Roles Onboarding Tracker is maintained to monitor role assignments, onboarding progress, and training completion.

Furthermore, discussion with management noted that training is also provided through discussions during working group meetings where updates are provided on processes if required. Our testing noted that training is not currently provided to the corporate domains as data governance processes have not been rolled out to these domains.

- **Data Governance Group (DGG)**
  Review of the Data Governance Group (DGG) meeting presentation packs from February, March, and June 2026 confirmed that there was oversight of data quality through reporting of data quality metrics, discussion and escalation of data quality issues, and agreed action plans to support remediation and accountability.



**Additional Information**

**We have identified the following issues during our fieldwork which we wanted to bring to the attention of management and the Audit and Risk Assurance Committee, although we have not raised a formal management action in relation to this issue.**

- **Data Dictionary**

Currently, the data dictionary only identifies and records the data assets for the regulatory domains; registration, fitness to practise and education. Management informed that these domains were prioritised due to their regulatory nature, and subsequently the data assets relating to the corporate domains (i.e. Human Resources, Finance and Partners) have not been identified and recorded in the data dictionary.

Due to limited capacity within the Data Governance Team, identifying data assets in the corporate domains will not be considered until work has been completed to resolve any issues identified with the data for the regulatory domains and once current processes have been strengthened.



# Summary of actions for management

# Summary of management actions

**The action priorities are defined as:**

**High:** immediate management attention is necessary

**Medium:** timely management attention is necessary

**Low:** there is scope for enhancing control or improving efficiency

| Ref | Management action | Priority | Responsible owner | Date |
|---|---|---|---|---|
| 1 | a) Management will identify the key data assets and domains to be monitored against the data quality dimensions defined within the data dictionary and agree appropriate performance metrics.<br>b) Monthly, performance against the metrics will be reported for each domain as part of the dashboard.<br>c) The dashboard will be discussed at the Data Governance Group meetings and escalated to an appropriate governance committee where required. | H | Esther Olanrewaju – Data Governance Lead | 31 March 2027 |
| 2 | Management will agree a due date for each data quality issue raised. At agreed intervals, Data Stewards will provide an update on the progress made to resolve any data issues.<br>Any overdue issues will be escalated to the Data Owner, and the number of overdue issues will be reported and discussed at the Data Governance Group. | M | Data Owners - Richard Houghton, Jamie Hunt, Jodie Summerfeld, Claire Baker and Leanne Silvestro | 31 March 2027 |
| 3 | At agreed intervals, the Data Governance Group will provide assurance to the Information and Technology Governance Board on performance against the agreed data quality metrics.<br>Where required, any issues will be escalated to the Executive Leadership Team for oversight and further discussion. | M | Gareth Davies - Head of Insight, Intelligence & Analytics | 31 March 2027 |
| 4 | The Data Governance Policy will be updated to include the next review date. Where material changes are made to the policy, the policy will be subject to approval by the Information & Technology Governance Board and / or an appropriate governance committee. | L | Gareth Davies - Head of Insight, Intelligence & Analytics | 31 December 2026 |

| Ref | Management action | Priority | Responsible owner | Date |
|---|---|---|---|---|
| 5 | Instances where responses are not received from the relevant Data Owner and/or Data Steward will be escalated to the Data Governance Group to provide oversight and accountability. | L | Geoff Kirk - Head of IT and Digital | 31 December 2026 |
| 6 | Where changes to roles or personnel occur within a domain, the Head of Department will re-assign the role of the Data Steward or Data Owner and will inform the Data Governance Team. Where changes are required, the Data Dictionary will be updated. | L | Esther Olanrewaju – Data Governance Lead | 31 December 2026 |



# Detailed findings and actions

# Agreed management action plan

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: Quality Metrics** | | | | | | |
|---|---|---|---|---|---|---|
| | | **Design** | X | **Application** | X | |
| **Missing Control** | The Health and Care Professions Council (HCPC) uses Power BI dashboards to monitor data quality across key domains, providing visibility of data quality dimensions. The data dictionary has mapped and identified the quality dimensions for each data asset however this is not reported and monitored for all quality dimensions. | | | | | |
| **Findings, risk and implications** | Data quality dimensions have been defined and mapped to data assets within the data dictionary. Whilst the dimensions have been identified for each data asset, compliance against this is not being monitored and reported. Review of the Data Quality Dashboards for the Registration, Education and Fitness to Practise domains found that monitoring is focused on completeness, with only the Registration dashboard including metrics relating to data validity. Other key data quality dimensions, including accuracy, consistency, uniqueness and timeliness, are not measured and reported. There is a risk that the quality of data is not measured so that appropriate actions can be taken to improve the quality of data.<br>There is a risk that management are unable to effectively monitor the quality of data to target remediation activities and make improvements, where required, to ensure that the data is accurate, complete and reliable for decision-making purposes. | | | | | |
| **Key audit theme(s)** | Design of the control framework | | | | | |
| **Management action 1** | a) Management will identify the key data assets and domains to be monitored against the data quality dimensions defined within the data dictionary and agree appropriate performance metrics.<br>b) Monthly, performance against the metrics will be reported for each domain as part of the dashboard.<br>c) The dashboard will be discussed at the Data Governance Group meetings and escalated to an appropriate governance committee where required. | **Responsible Owner:** Esther Olanrewaju – Data Governance Lead | **Date:** 31 March 2027 | **Priority** | H | |

| Area: Stewardship and Data Quality Issues | | | | | |
|---|---|---|---|---|---|
| | | Design  | | Application  | |
| **Control** | Microsoft Lists is used to track data quality issues and assign them to the relevant Data Stewards for investigation and remediation. Progress is monitored and recorded until issues are resolved and affected records are corrected. | | | | |
| **Findings, risk and implications** | We conducted a walkthrough of Microsoft Lists and reviewed the Data Quality Issue Extracts for the Registration, Education, and Fitness to Practise domains. Review confirmed that issues are recorded with key information, including priority, owner, ageing status, target date, and status. However, target dates were not consistently achieved, resulting in a significant number of overdue issues and we noted that some issues remained open for over 100 days.<br><br>Although issues are assigned to Data Stewards and corrective actions recorded, there was limited evidence of progress updates particularly within the Education and Fitness to Practise domains. In addition, the escalation field within the tracker had not been populated. There is a risk that data quality issues may not be consistently monitored, escalated, and resolved in a timely manner, increasing the risk of prolonged data inaccuracies and recurring data quality issues. Management informed us that issues have remained open due to system fixes and internal discussions. However, the Microsoft List was not updated to reflect that the delays related to system fixes, limiting transparency and potentially reducing the reliability of management information used for decision-making. | | | | |
| **Key audit theme(s)** | Poor record keeping | | | | |
| **Management action 2** | Management will agree a due date for each data quality issue raised. At agreed intervals, Data Stewards will provide an update on the progress made to resolve any data issues.<br><br>Any overdue issues will be escalated to the Data Owner, and the number of overdue issues will be reported and discussed at the Data Governance Group | **Responsible Owner:**<br>Data Owners - Richard Houghton, Jamie Hunt, Jodie Summerfeld, Claire Baker and Leanne Silvestro | **Date:**<br>31 March 2027 | **Priority**  | |

| Area: Information and Technology Governance Board | | | Design ✓ | Application X |
|---|---|---|---|---|
| **Control** | Information and Technology Governance Board meetings are held on a quarterly basis, supported by subgroups, to provide oversight of data governance and data quality through defined accountability, escalation, and reporting arrangements. | | | |
| **Findings, risk and implications** | The Information and Technology Governance Board (ITGB) met in February and June 2026, and management informed that there have been two meetings since the Board was established this year.<br><br>Review of the minutes from the meetings held in February and June 2026 confirmed that the ITGB receives updates from the data governance group (DGG) however this was at a high level. Furthermore, review noted that it was not clear whether the ITGB reviews data quality metrics, data quality reports, or remediation activities. In addition, escalation for significant data quality issues and risks was inconsistently discussed.<br><br>There is a risk that data quality issues and remediation activities are not escalated and reported from the DGG to the ITGB, limiting effective oversight. | | | |
| **Key audit theme(s)** | Governance weakness | | | |
| **Management action 3** | At agreed intervals, the Data Governance Group will provide assurance to the Information and Technology Governance Board on performance against the agreed data quality metrics.<br><br>Where required, any issues will be escalated to the Executive Leadership Team for oversight and further discussion. | **Responsible Owner:**<br>Gareth Davies – Head of Insight, Intelligence & Analytics | **Date:**<br>31 March 2027 | **Priority** M |

| Area: Governance - Executive Leadership Team | Design ✓ | Application X |
|---|---|---|
| **Control** | Data Governance & Data Quality updates are presented to the Executive Leadership Team (ELT) to monitor data quality and compliance to support data governance oversight and reporting. | |
| **Findings, risk and implications** | Data governance and data quality updates are reported monthly to the Executive Leadership Team (ELT) to support oversight of data quality. However, our review of updates presented at the meetings held in March, April and June 2026 identified inconsistencies in reporting of metrics. Whilst the update presented at the meeting in March included information on data quality issues and dashboard metrics, the update presented at the meeting in April did not include any data quality metrics or measurable performance information. Management informed that the metrics were omitted as there were no issues with the data quality performance.<br><br>Without consistent reporting of key metrics, there is a risk that the ELT may not have sufficient oversight of data quality. **Refer to management action 3.** | |

| Area: Data Governance Policy | Design ✓ | Application X | | |
|---|---|---|---|---|
| **Control** | The Data Governance Policy and Procedure is in place and defines principles, roles, and governance structures to ensure data quality and governance are effectively managed. | | | |
| **Findings, risk and implications** | There is a Data Governance Policy in place which is dated September 2025. Review of the Policy confirmed that the governance principles, roles and responsibilities, oversight arrangements, data quality standards, issue management processes, and monitoring requirements are outlined. However, review noted that the policy does not state the next review date or the governance committee responsible for approving the policy. Although, review of email correspondence dated September 2025 noted that the policy was approved by the Head of Insight & Analytics and the Head of IT and Digital in August and September 2025. Management informed that whilst the policies were developed as part of the Data Governance Programme, they were not formally presented for approval at the Data Governance Group (DGG) meetings and instead the draft documents were circulated to the Data Governance members outside of the committee meeting for review and feedback. There is a risk that policies may not be reviewed and updated on a timely basis, which could result in the incorrect processes being followed. | | | |
| **Key audit theme(s)** | Policies and procedures | | | |
| **Management action 4** | The Data Governance Policy will be updated to include the next review date. Where material changes are made to the policy, the policy will be subject to approval by the Information & Technology Governance Board and / or an appropriate governance committee. | **Responsible Owner:**<br>Gareth Davies – Head of Insight, Intelligence & Analytics | **Date:**<br>31 December 2026 | **Priority** L |

| Area: Procedural Documentation | Design  | Application  |
|---|---|---|
| **Control** | HCPC maintains data quality management documents that define data quality principles, controls, roles and responsibilities, and governance arrangements. | |
| **Findings, risk and implications** | We reviewed the following policies:<br>• Data Quality Issue Management issued in September 2025.<br>• Data Quality Management issued in September 2025.<br>• Data Quality Standards and Procedures issued in September 2025.<br>Review of the policies and procedures noted that the next date of review was not recorded, along with the governance group and /or committee that approved the policies and procedure documents. Management informed that these documents were circulated to the DGG for review and comment outside of the meeting. There is a risk that policies may not be reviewed and updated on a timely basis, which could result in the incorrect processes being followed. **Refer to management action 4.** | |

| Area: Data Access | | | | | |
|---|---|---|---|---|---|
| | | Design | ✓ | Application | X |
| **Control** | On a quarterly basis, the IT team reviews network user access rights for each domain. Data Owners or Stewards are required to confirm that access rights are appropriate. | | | | |
| **Findings, risk and implications** | Review of email correspondence circulated by IT to the Data Owner or Data Steward for each regulatory domain in March and June 2026 noted that each Data Owner / Data Steward was required to review the access rights for their domains and confirm the accuracy of the information. However, there were two instances where the Registration and Fitness to Practise (Tribunal Service) domain could not evidence that they had reviewed and responded to the audit which was undertaken in March 2026. There is a risk that individuals may have access to data when access is no longer required. | | | | |
| **Key audit theme(s)** | Poor record keeping | | | | |
| **Management action 5** | Instances where responses are not received from the relevant Data Owner and/or Data Steward will be escalated to the Data Governance Group to provide oversight and accountability. | **Responsible Owner:** Geoff Kirk – Head of IT and Digital | **Date:** 31 December 2026 | **Priority** | L |

| Area: Accountability | | | | | |
|---|---|---|---|---|---|
| | | Design |  | Application |  |
| **Control** | Every Data Asset is assigned a Data Owner for strategic oversight and proper use of data, and a Data Steward is responsible for day-to-day data management and quality activities. | | | | |
| **Findings, risk and implications** | For a sample of 20 data assets, review of the data dictionary confirmed that each data asset was assigned a Data Owner and Data Steward. However, we noted that there were seven instances where the Data Steward recorded in the data dictionary had left the HCPC at the time of our audit, and it was noted that the dictionary had not been updated to reflect these changes. Discussion with management informed that currently this role is vacant and the role of the Data Steward will need to be re-assigned. Currently, the Data Owner for this domain has taken on the responsibility of the Data Steward. There is a risk that the roles responsible for managing data are not accurate, which could lead to a lack of accountability. | | | | |
| **Key audit theme(s)** | Poor record keeping | | | | |
| **Management action 6** | Where changes to roles or personnel occur within a domain, the Head of Department will re-assign the role of the Data Steward or Data Owner and will inform the Data Governance Team. Where changes are required, the Data Dictionary will be updated. | **Responsible Owner:** Esther Olanrewaju – Data Governance Lead | **Date:** 31 December 2026 | **Priority** | L |



# Appendices

# Appendix A: Internal audit assignment opinions

## Categorisation of internal audit findings

- **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 licenses or material fines.
- **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.
- **Low:** there is scope for enhancing control or improving efficiency.






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).



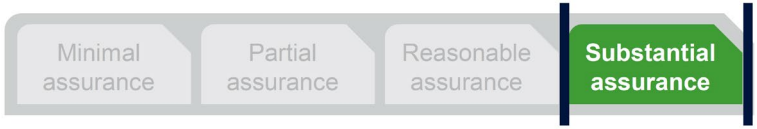

Taking account of the issues identified, the board can take partial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

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



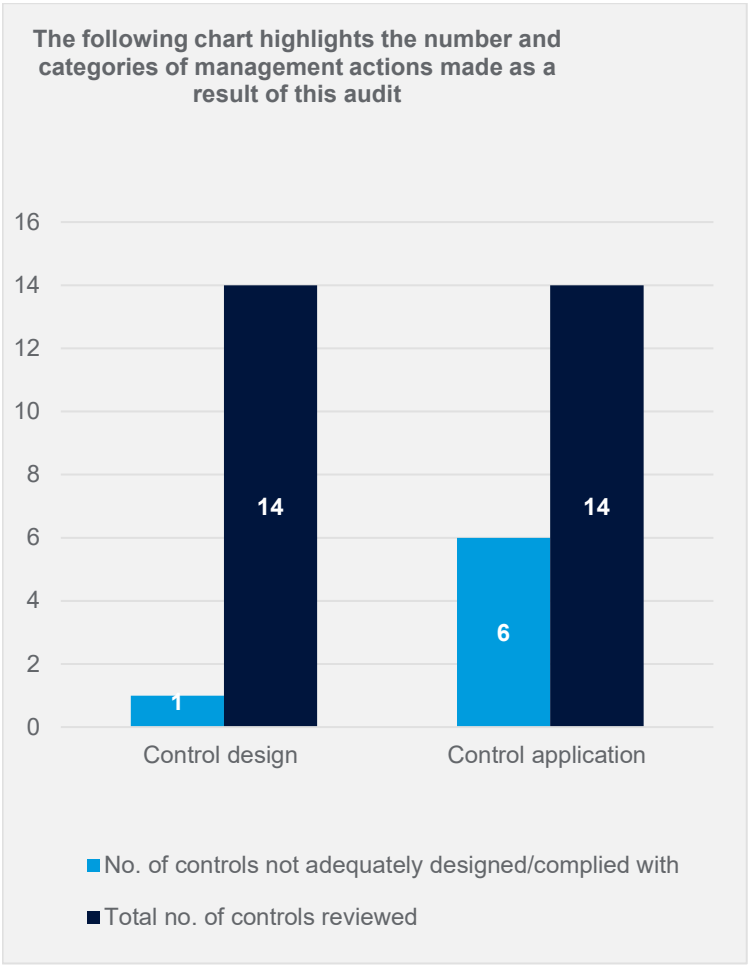

Taking account of the issues identified, the board can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

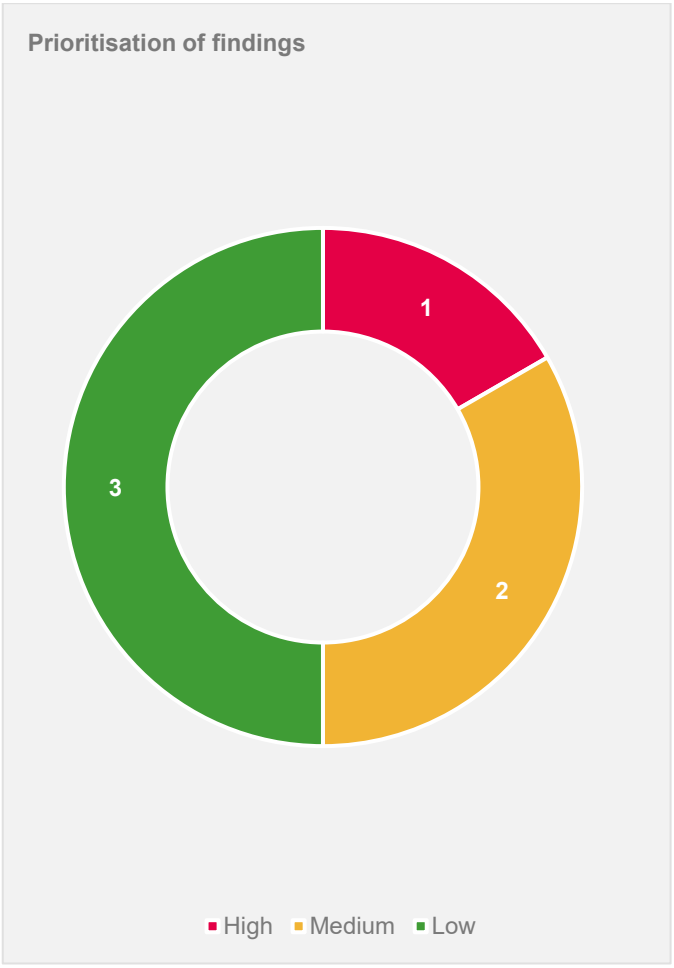
However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk(s).

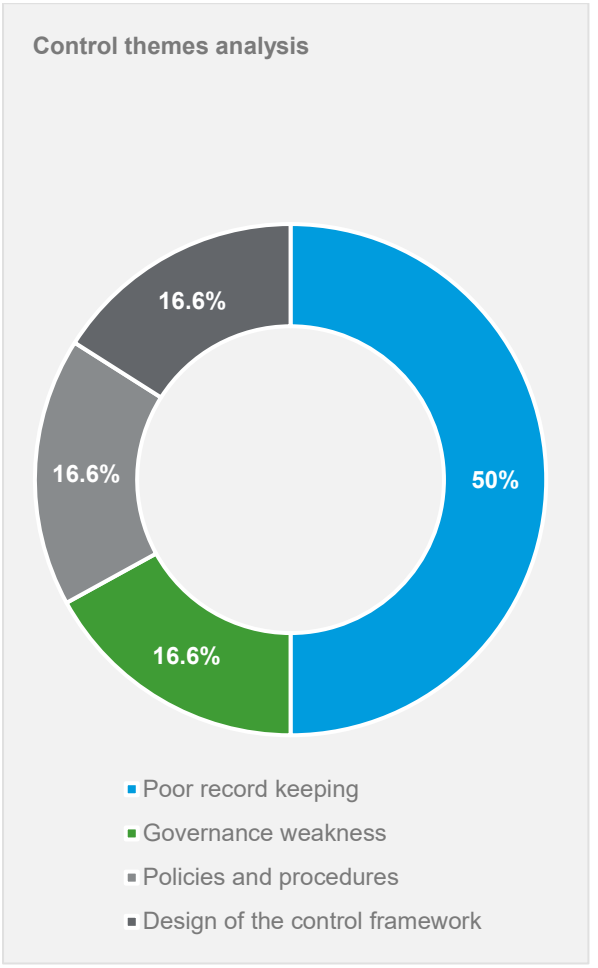



Taking account of the issues identified, the board can take substantial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

# Appendix B: Summary of findings



# Appendix C: Scope

We confirm that, to the best of our knowledge, everyone involved in this engagement was free from any personal or other impairments that would affect their ability to plan, deliver or report on this review objectively and independently.

## Scope of the review

The scope was issued to management on 19 May 2026 and planned to provide assurance on the controls and mitigations in place relating to the following:

| Objective of the review | Assignment approach | Strategic objective or Strategic risks relevant to the scope of the review | Risk source |
|---|---|---|---|
| To provide assurance over the robustness of processes and systems in place surrounding data collection, preparation, review and reporting to ensure accuracy of key activity and performance data. | Risk based | Inadequate data processes and controls may lead to inaccurate performance data being reported and relied upon. | Business Risk |

## When planning the audit, the following were agreed:

In 2025, the Executive Leadership Team agreed data governance principles which are outlined in the Data Governance Framework / Policy. The Framework / Policy aimed to ensure that there was robust processes in place to effectively manage enterprise data at the organisation.

**Areas for consideration:**

- Whether there are policies in place relating to data quality and data governance which have been subject to approval by an appropriate governance committee and is reviewed timely.
- We will consider how data is stored, who is able to access the data and the retention period for data.
- Data is entered onto the system by appropriate personnel who have been suitably trained.
- We will agree the data assets which are to be reviewed with management and we will test compliance with the data governance principles outlined in the Data Governance Policy specifically focussing on:
    - Accountability – each data asset has an assigned data owner and data steward.
    - Transparency – data definitions, business rules and / or standards are documented and accessible.
    - Quality – data is complete, timely, accurate, consistent and fit for purpose.
    - Stewardship – there is a process for ensuring data quality standards are upheld and data issues are addressed.

- Assess whether governance and reporting arrangements enable effective oversight of data quality through clear accountability, escalation, and reliable reporting.
- Whether there adequate and automated tools in place to check and monitor the quality of data.

**Limitations to the scope of the assignment:**

- The scope of the work is limited to those areas examined and reported upon in the areas for consideration in the context of the objectives set out for this review.
- Testing will be undertaken on a sample basis only from the last six months.
- We will not consider the organisation's entire control framework in relation to data quality and we will not provide an assurance opinion on the entire control framework.
- Our review will not consider the validity of decisions made attributing to the data. Our review only considers the accuracy of how the data is recorded.
- We will not provide assurance on whether data governance process are compliant with applicable laws and regulations i.e. GDPR, ISO27001, cyber essentials plus and internal data protection and IT security policies.
- Our review may involve interviews with a sample of staff, and as such, conclusions will be drawn from our discussions.
- The results of our work including data analytics work is reliant on the quality and completeness of the information provided to us.
- Our work will not provide an absolute assurance that material errors, loss or fraud do not exist.

| | | | |
|---|---|---|---|
| **Debrief held** | 31 July 2026 | **Internal audit contacts** | Nick Atkinson – Head of Internal Audit<br>Sarah Howe – Associate Director<br>Clara Agyekumhene – Managing Consultant<br>Farrell D'Mello – Consultant |
| **Draft report issued** | 18 August 2026 | | |
| **Responses received** | 4 September 2026<br>23 September 2026<br>1 October 2026 | **Client sponsor** | Andrew Smith – Deputy Chief Executive and Executive Director of education, Registration & Regulatory Standards |
| **Final report issued** | 5 October 2026 | **Distribution** | Andrew Smith – Deputy Chief Executive and Executive Director of education, Registration & Regulatory Standards<br>Gareth Davies – Head of Insight, Intelligence and Analytics<br>Geoff Kirk – Head of IT and Digital<br>Esther Olanrewaju – Data Governance Lead |

**THE POWER OF BEING UNDERSTOOD**
AUDIT | TAX | CONSULTING

RSM

For further information please contact:




## Nick Atkinson

Head of Internal Audit

**E:** Nick.Atkinson@rsmuk.com

**T:** +44 (20) 32018028





## Sarah Howe

Associate Director

**E:** Sarah.Howe@rsmuk.com

**T:** +44 20 3201 8773


**rsmuk.com**


The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of The Health and Care Professions Council (HCPC) and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Consulting for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Consulting will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

**RSM UK Consulting**

RSM UK Consulting is a trading name. If the subject matter of this report relates to an engagement with RSM UK Consulting LLP (registered number OC397475), RSM UK Corporate Finance LLP (registered number OC325347), RSM UK Risk Assurance Services LLP (registered number OC389499) or RSM UK Tax and Accounting Limited (registered number 06677561) this report is sent on behalf of that entity. In all other cases, this report is sent on behalf of RSM UK Tax and Consulting LLP (registered number OC325348). These limited liability entities are registered in England and Wales with their registered office at 6th Floor 25 Farringdon Street, London, EC4A 4AB.