BDO

Health and Care Professions Council

Follow Up

Internal Audit Report – Final

June 2026

IDEAS | PEOPLE | TRUST

Contents

Distribution List	
For Action	Anna Raftery, Head of Quality Assurance
	Nicole Jones, Improvement and Compliance Specialist
For Information	ARAC

Report Status	
Lead Auditor:	Maciej Grzech
Reviewed By:	Joshua Wilson, Manager Bill Mitchell
Dates Work Performed:	16 February to 11 May 2026
Draft Report Issued:	26 May 2026
Management Responses Received:	28 May 2026
Final Report Issued:	2 June 2026

Executive Summary

Overview

Background

This audit was completed in accordance with the approved annual Internal Audit plan for 2025/26. The implementation of internal audit recommendations is an important part of an organisation's internal control framework. This review is a follow-up of BDO's internal audit recommendations and agreed actions which were marked as completed across the four ARAC meetings since the last round of follow up. A total of thirteen medium priority recommendations across seven internal audit reports were reviewed. Evidence was requested to determine implementation.

Acknowledgement

We appreciate the assistance provided by the staff involved in the review and would like to thank them for their help and ongoing cooperation.

Methodology

The Internal audit reports from which the recommendations being followed-up on are drawn are:

- Regulatory Policy
- Unified Assurance Framework
- Procurement of Large Contracts
- Project Management
- Data Privacy
- Stakeholder Engagement
- Diversity

Audit Area	Total high	Total medium	Total low	Total included in review
Regulatory Policy	-	1	-	1
Unified Assurance Framework	-	2	-	2
Procurement of Large Contracts	-	2	-	2
Project Management	-	2	-	2
Data Privacy	-	4	-	4
Stakeholder Engagement	-	1	-	1
Diversity	-	1	-	1
TOTAL	**-**	**13**	**-**	**13**

Executive Summary

Overview

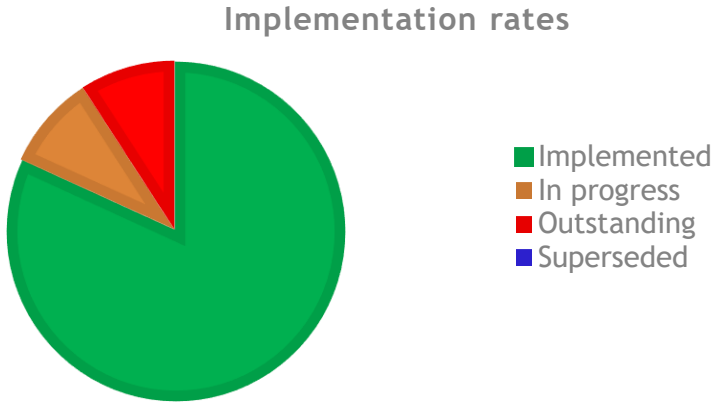
Results

Of the thirteen recommendations tested during this review, eleven recommendations were fully implemented, representing 85% of the recommendations tested. Of the remaining recommendations, one was in progress and one was outstanding, with no current planned action being taken to address the recommendation. All recommendations were classified as Medium priority.

For the medium outstanding recommendation, the procurement-related recommendation concerned the absence of a formal spot-check process over procurement activity. The remaining recommendation related to mandatory training compliance is in progress, and related to where automated reminders are in place, but there is no formal reporting schedule or disciplinary measures for non-completion.

Overall, progress is positive, but more work is required to fully close out all recommendations. Management may also benefit from a sense check of responses provided before marking recommendations as closed.

Audit	BDO Status as at May 2026 (definitions included within Appendix III to the report)				Total
	Implemented	In progress	Outstanding	Superseded	
Regulatory Policy	1	-	-	-	1
Unified Assurance Framework	2	-	-	-	2
Procurement of Large Contracts	1	-	1	-	2
Project Management	2	-	-	-	2
Data Privacy	4	-	-	-	4
Stakeholder Engagement	1	-	-	-	1
Diversity	-	1	-	-	1
TOTAL	**11**	**1**	**1**	-	**13**



Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
1	Regulatory Policy	HCPC should align its risk assessment for individual consultations directly to the strategic risk register and report this in its papers to ELT and the Council. The paper should set out whether the subject matter risk sits within the risk appetite or outside of the risk appetite. Where the consultation subject matter sits outside, HCPC should consider whether additional controls are required such as what additional actions will be undertaken because of the risk assessment. HCPC can also consider the 'phrasing' of consultations to ensure appropriate for the risk and to enable stakeholder buy-in.	Working with Governance, discuss how we might include risk assessment and risk appetite within governance paper cover sheets across the organisation.	Medium	HCPC has introduced an updated paper template for submissions to the Executive Leadership Team and Council, which includes an executive summary and requires authors to set out the rationale for submission to these bodies. The template includes sections covering strategic priorities, associated strategic risks, and the relevant risk appetite, enabling individual consultation papers to be explicitly aligned to the strategic risk register and assessed against the organisation's stated risk appetite. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
2	Unified Assurance Framework	Following implementation of recommendations 1-4, The Quality Assurance Team should introduce a rolling programme of reviews of team assurance maps over a three-year cycle, assessing the veracity of the self-assessment statements and providing and independent assessment of the strength of the control environment (Year 2). As part of the above process, collate information on best practice observed and use this to continually improve the good practice guidance and Quality Framework (Year 2).	Departmental self-assessment statements and methods will be evaluated on a case-by-case basis, to check the veracity of claimed effectiveness, and share best practise where observed and applicable to other departments.	Medium	Management agrees with the intent of the recommendation but has chosen to address the underlying risk through a risk-based Quality Assurance (QA) workplan rather than a structured, time-bound rolling review programme. This alternative approach is considered to meet the intent of the original recommendation. The Internal QA Workplan for 2026-2027 was provided and sets out planned assurance activity across key focus areas, aligned to the assurance framework. The workplan outlines specific review topics, priorities, timelines, and assigned leads covering the period from April 2026 to April 2027. Good practice documentation was provided and is updated where appropriate, informed by self-assessments and reported to the Executive Leadership team. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
3	Unified Assurance Framework	Develop a Quality Framework that contains 'pillars' to create a standard way in which to assess the control environment across departments. These pillars could include Policies and Guidance, Induction and Training, Quality Checks / Peer Review, Continuous Improvement and Performance Monitoring, as examples (Year 1). For each pillar, design high level guidance setting out expectations for the expected controls to be captured within each pillar, including a good/better/best system of self assessment to support continuous improvement (Year 1). Ask teams to complete a self-assessment against each of the pillars, utilising the good practice guidance. Collate these responses and use them as the basis for the population of the UAF (Year 2).	The variability of level 1 assurance activity across departments reflects the existing matrix of departmental workload, resources, processes and stability of those variables. Level 1 check enhancement may require resources greater than those possible under existing financial constraints. However, efforts to include these potential pillars will continue and progress to deliver against these pillars will be monitored.	Medium	HCPC has developed a Quality Framework structured around defined pillars to support a consistent assessment of the control environment across departments. The Unified Assurance Framework (UAF) 2025-26 sets out these pillars as: documented guidance and processes, training and induction, KPIs and reporting, quality checks, and business continuity. For each pillar, guidance has been established outlining the expected controls and key assessment questions. Teams complete self-assessments against these pillars using a standardised rating scale that defines levels of assurance. The completed self-assessments are collated and used to populate the UAF. The UAF includes all teams, with quarterly ratings recorded consistently across the organisation. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
4	Procurement of large contracts	The Procurement team should: Introduce second line and documented 'spot checks' to ensure that procurement activity is in line with prescribed guidance. 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. Introduce a more comprehensive description of any large value contracts single source requests with a focus on the effectiveness of the procurement process.	The QA team will be engaged via the entire procurement process for large contracts through emails, meetings and/or MS Teams to increase visibility of relevant documents, approvals and other issues. This will give them the opportunity to raise any concerns throughout the entire process and ensure that we are collaborating every step of the way.	Medium	Procurement activity is undertaken within the Procurement function, with no formal QA-led spot check process currently embedded. Oversight is provided through management engagement and approvals, and adherence to the procurement policy. While supporting checks are performed by other functions as part of the process, such as ad-hoc involvement from the Chief of Information Security, to conduct data security checks where required, these activities are not formally structured or evidenced as independent spot checks. Managements view is that getting the QA team to conduct spot checks is challenging due to the detailed procurement knowledge required. It would be appropriate however, for procurement to conduct these checks if independent from the specific tender. **Outstanding**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
5	Procurement of large contracts	HCPC should ensure that: On at least an annual basis employees are reminded to review and update their Conflict of Interest (COI's) declarations. There is documented evidence for each procurement activity that potential conflicts of interest have been considered.	Conflict of interest declaration forms are completed by all tender panel members and relevant stakeholders during the process, regardless of the contract value. These forms are stored as part of the tender records and are now a key requirement for all tenders, which needs to be stipulated in the revised Procurement Manual.	Medium	Conflict of interest declarations are completed as part of procurement activities, with individuals formally declaring any actual or potential conflicts in advance of tender exercises. Declarations include confirmation of the presence or absence of conflicts, they are formally signed, dated and linked to relevant procurement exercise. Conflicts are appropriately managed through safeguards such as observer-only participation in the evaluation process. During this follow up review, it was noted annual COI reminders were not sent (although this was completed upon prompting from this review). However, as part of each procurement exercise a conflict-of-interest declaration is due to be made and this was evidenced from a procurement. This sufficient mitigates the risk. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
6	Project Management	During benefits review, at each stage of the project lifecycle, project teams and the review panels (especially the Change and Benefits Forum) should ensure that projects focus on citing the final outputs, define more exactly what success means and prioritise benefits into 'key benefits' and 'other'.	We can link the benefits against the 'must' scope items which will mean they're the key deliverables. Regarding defining what success means, this detail will be part of the requirements outputs, and has an agreed acceptance criteria rather than the investment case. we will agree to link this when carrying out the investment prioritisation for FY 25/26.	Medium	Project business cases include defined objectives, success criteria, and documented benefits linked to intended outcomes. Benefits are recorded within a structured register, supported by information on delivery status, timing, and performance measures. This is complemented by defined monitoring attributes, including corresponding report name, realisation date, assigned owner, status, and target measurement, which support ongoing reporting throughout the project lifecycle. Benefits are prioritised using an agreed methodology. However, benefits are categorised by scope and delivery impact rather than being explicitly distinguished as 'key benefits' and 'other', as set out in the recommendation. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
7	Project Management	Clarify the authority of the Change and Benefits Group, particularly whether it recommends investment cases to ELT for ELT approval. It would also be useful to clarify its authority over live projects. Alternatively, HCPC should stand up an investment committee to conduct the approval on behalf of the board (i.e. Council).	We accept this recommendation and will update the TOR to clarify the role of the CBF.	Medium	An updated Terms of Reference is now in place for the Change Benefits Forum, which set out its role in reviewing investment cases and recommending them to the Executive Leadership Team for approval. The Forum is defined as an advisory body, providing assurance on strategic alignment and benefits identification, with final approval decisions taken by the Executive Leadership Team. The ToR clarifies the Forum's role in relation to live projects, with delivery accountability retained by individual Project Boards. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
8	Data Privacy	HCPC should reconfigure the RoPA to document; a) Purpose of processing b) Data processed c) Categories of data subjects d) Single most appropriate lawful basis for processing e) Additional conditions for special category data f) Name of third-party data processors and joint controllers g) Locations of third-party data processors and joint controllers h) Systems in which personal data is stored.	We accept the findings. Elements a)-h) will be documented in the Risk Info Assets document.	Medium	A Record of Processing Activities (RoPA) is in place as a centrally stored Excel-based register. It documents the purpose of processing, the data processed, categories of data subjects, the most appropriate lawful basis for processing, the names and locations of third-party data processors and joint controllers, and the systems in which personal data is stored. Note that additional conditions for special category data are not applicable, as HCPC does not process such data. **Implemented**	
9	Data Privacy	Incorporate version control in the RoPA to evidence regular review and to ensure that the RoPA is updated on an on-going basis (at a minimum annually).	We accept the findings. A version control tab will be incorporated in the Risk Info Assets document.	Medium	A document control history is in place for the Record of Processing Activities (RoPA), evidencing the most recent updates. The version control is incorporated as a separate tab within the RoPA Excel spreadsheet and shows reviews and changes were made in 2025 and 2026. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
10	Data Privacy	HCPC should update the data subject rights procedure to include: • The process to follow when any data subject rights requests is received (such as the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling). • Key timescales for completion i.e. as soon as possible or within one calendar month (extended by a further two month in certain circumstances). • Version control details to evidence regular review.	We accept the findings. The process for managing all types of data subject rights requests will be updated. The procedure will be updated to reference key timescales for completion and version control.	Medium	The Data Protection Policy has been updated to set out all required aspects. The policy outlines the process for submitting requests, specifies statutory response timescales of one calendar month (with provision for extension by a further two months where appropriate), and provides a dedicated contact email for requests. The document includes version numbering, however, there is no version history tracking to evidence regular review. In addition, a separate procedure, SEC InfoGov-GDPR Rights for Individuals, is in place and documents a detailed, three-stage process for receiving, processing, and responding to data subject rights requests. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
11	Data Privacy	HCPC should promote the data subject rights process internally by: • Incorporating the process (for reporting rights requests internally) in mandatory training. • Periodic employee awareness initiatives to remind them of internal processes when a data subject rights request is received. • Asking team leaders to cascade information about the process to their teams.	We accept the findings. The process for recognising and escalating SARs is included in mandatory training which is being rolled out (February 2025). Intranet post raising awareness of SAR processes will be published. Team Leaders will be contacted to cascade this information to their teams. Furthermore, specific departmental training is planned for roll out in August 2025	Medium	The data subject rights process is promoted internally through mandatory information security training, covering statutory deadlines and internal reporting routes. Periodic awareness initiatives are also in place, including information governance presentations and corporate induction materials that address data subject rights. Responsibility for promoting awareness of the process currently sits centrally with the Chief Information Security and Risk Officer, whilst team leaders are not asked to cascade information to their teams. This is considered a more efficient and effective mechanism given the technical nature of the subject matter. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
12	Stakeholder Engagement	Review and update the arrangements in place with Luther Pendragon for the management of stakeholders for HCPC. The expectations should be set and documented and include who Luther Pendragon report to, the remit of their role, where they record information, set timeframes and key performance indicators (KPIs) for stakeholder management.	We believe additional clarity in our stakeholder response would be beneficial to all parties, including our outsourced supplier. Alongside a wider stakeholder documentation, a specific requirements document is being created to ensure clarity for our outsourced supplier and internal colleagues.	Medium	Arrangements with Luther Pendragon are documented and set out within agreed Ways of Working, which define reporting lines, roles and responsibilities, and expected timeframes for delivery. Luther provides communications support rather than undertaking activity directly, with outputs that are used to inform HCPC stakeholder records and briefings. While roles, reporting arrangements, and timeframes are documented, no KPIs are currently defined for stakeholder management, as this function is no longer carried out beyond logistical arrangements. **Implemented**	

Appendix I - Recommendations Summary

Ref.	Report Area	Original Recommendation	Management Response	Priority	Status Update	Rec. Status
13	Diversity	We recommend that: • Staff members with training outstanding are encouraged to complete their required training as soon as possible. • A fixed schedule is set for reporting on training completion rates to the HoDs and the ELT. • Disciplinary procedures should be formally implemented for any staff members who do not complete staff training in the required time frame. • A formal sanction process is implemented if a partner does not attend their induction and complete outstanding ED&I training.	A document was provided stating that 17 staff from a total of 336 had not completed EDI training by the required deadline. Some instances included staff returning from maternity leave and staff on career breaks. However, there were several instances where it was not clear why training had not been completed, nor the action being taken to complete the training. Whilst it may not be possible to have all staff 100% up to date at any one time, reasons should be identified for those staff who are at work but have not completed the training. We were informed that quarterly reviews of training completeness are undertaken, which include first and secondary checks. The L&D team proactively engage with people who have not completed training, and their line managers are also made aware that training should be completed	Medium	Automated email reminders are issued via the LH system to staff with outstanding mandatory Equality, Diversity & Inclusion training. At the time of the original audit, 260 staff members were non-compliant, representing a 31% completion rate across the organisation. However, as a result of work undertaken by the L&D team, at the time of follow up completion rates had increased to 97%. There is no fixed schedule for reporting training completion rates to Heads of Department or the Executive Leadership Team, and no formal disciplinary provisions apply to employees for non-completion. For partners, training requirements are formally documented within the Partner Training Guidance, with induction and refresher training mandatory under the code of Conduct, and that non-compliance may result in immediate termination of contract. **In progress**	

Appendix II - Staff Interviewed & follow up definitions

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.	
Anna Raftery	Head of Assurance and Compliance
Nicole Jones	Improvement and Compliance Specialist
Ifeoluwa Ojo	Procurement Manager
Roy Dunn	Chief Information Security and Risk Officer
Matthew Peck	Head of Communications and Engagement
Paul Cooper	Head of Business Change
Edin Kekic	Procurement Business Partner

Recommendation Status	
Implemented	
In Progress	
Outstanding	
Superseded	
Risk Accepted	

Appendix III: Limitations and Responsibilities

Management Responsibilities

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

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

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

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

Limitations

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

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

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

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

Conformance with the Global Internal Audit Standards

This engagement has been conducted in accordance with the Institute of Internal Auditors' Global Internal Audit Standards.

FOR MORE INFORMATION:

Bill Mitchell, Director

Bill.Mitchell@bdo.co.uk

Sarah Hillary, Partner
Sarah.Hillary@bdo.co.uk

www.bdo.co.uk

42001482

Health and Care Professions Council (HCPC)

Risk Management

Internal Audit Report - Final

June 2026

Level of Assurance:	
Design	Limited
Effectiveness	Limited

IDEAS | PEOPLE | TRUST

BDO

Contents

Distribution list		
For action	Anna Raftery	Head of Assurance and Compliance
	Roy Dun	Chief Information Security & Risk Officer
	Nicole Jones	Improvement & Compliance Specialist
For information	Claire Amor	Executive Director of Corporate Affairs
	Audit Committee	

Report status	
Lead auditor(s):	Shamail Afroz
Dates work performed:	27 January - 12 March 2026
Additional documentation received:	23 April 2026
Draft report issued:	29 April 2026
Management responses received:	29 May 2026
Final report issued:	1 June 2026

Executive Summary

Level of assurance: (see Appendix I for definitions)		
Design	**Limited**	System of internal controls is weakened with system objectives at risk of not being achieved.
Effectiveness	**Limited**	Non-compliance with key procedures and controls places the system objectives at risk.

Summary of findings (see Appendix II)			# of agreed actions
H	0		
M	4		8
L	0		
Total number of findings: 4			

Purpose

The purpose of the review was to provide assurance over the control design and effectiveness of key risk management controls in operation at HCPC.

Background

As part of the agreed internal audit plan for 2025/26, as approved by the Audit and Risk Assurance Committee (ARAC), we were due to undertake a review of Risk Management. However, as this area was not ready for review, it was agreed with management and the ARAC that a review of key controls in respect to Risk Management would be conducted as the alternative.

Risk management is an important function for supporting an organisation in making key strategic decisions that are aligned to its risk tolerance. The practice of strong risk management supports the monitoring of activities, compliance with regulation and the maintenance of financial performance.

HCPC maintains both a Strategic Risk Register (SRR) and an Operational Risk Register (ORR). The SRR is owned by the Head of Assurance and Compliance and is reviewed by the Executive Leadership Team (ELT) and ARAC on a quarterly basis. While updates are made regularly, the last formal structured review of the strategic risks themselves was undertaken in November 2024, and the organisation intends to conduct a full review once the new Corporate Strategy is finalised in 2026.

The ORR is overseen by the Chief Information Security & Risk Officer and is submitted to ARAC annually. Individual departmental meetings take place quarterly to discuss risk-related activity and inform the ORR.

Each Risk Register lists the inherent, residual and target risks aligned to risk appetite. The appetite was last updated in 2023 and there is an expectation that this will be reviewed in 2026.

Controls and mitigating actions are recorded within both registers, however, the level of detail and evidence supporting these controls varies significantly. In many cases, assurance relies heavily on verbal updates from risk owners, with limited documentation to demonstrate that controls are operating effectively. Where future actions are noted, these are not always clearly tracked, assigned, or monitored through a consistent process.

Conclusion

Overall, HCPC has established several core components of effective risk management, including defined risk registers, clear ownership, and regular review through senior management and committee forums. These provide a foundation for effective risk management and demonstrate organisational commitment to managing risk.

However, the review identified that risk management arrangements are not yet operating in a sufficiently consistent or integrated manner to provide strong assurance. Key weaknesses include the absence of a documented Enterprise Risk Management (ERM) framework, an overly populated and low-quality ORR, unclear risk escalation arrangements, and insufficient documentation and monitoring of key controls and mitigating actions. Risk appetite is also not applied consistently, limiting assurance that risks are being managed within agreed tolerance levels.

Based on the work performed, we are able to provide Limited assurance over the design and Limited assurance over the effectiveness of HCPC's risk management controls.

Executive Summary

Summary of good practice

- Risk ownership is clearly assigned at both strategic and operational levels, with Executive Directors typically owning strategic risks, and Heads of Department owning operational risks.
- Risk appetite, last reviewed in 2023, is clearly defined for each directorate and is embedded it into the SRR, committee cover sheets and decision-making processes.
- A risk scoring matrix is clearly defined, with documented definitions of likelihood and impact, including impact scales that incorporate financial considerations such as estimated cost exposure and potential fines.
- Project-specific risk registers are in place for major business-change initiatives, providing more detailed risk monitoring for complex programmes
- Positive and negative risk influencers are captured within the SRR, ensuring the broader environment is reflected even when not creating standalone risks.
- A quarterly Unified Assurance Report is provided to ARAC with a consolidated snapshot of assurance coverage across the organisation, supported by an assurance map, risk appetite statement and workplans (including Quality Assurance and Internal Audits).

Summary of key findings

We identified four medium significance findings as part of our review. These related to the following:

- **Documented ERM Framework:** HCPC has an Operational Risk Management Policy; which serves as a ERM framework; however, it lacks key components of a comprehensive ERM Framework setting out a unified, organisation-wide approach to identifying, assessing, monitoring, and escalating risks. While strategic and operational risks are owned and discussed through established forums, the underlying processes rely heavily on informal discussions and individual judgement rather than standardised methodologies and documented evidence. This has resulted in inconsistent risk identification and assessment practices, limited evidence trail, and insufficient clarity over how risks are escalated, reviewed, and closed across the organisation.
- **Excess volume and data quality issues in the ORR:** The ORR contains an excessively high volume of risks and exhibits significant data-quality weaknesses, reducing its effectiveness as a prioritisation and governance tool. Risks are not consistently articulated, categorised, or aligned to risk appetite, and many, control implementation target dates, or defined criteria for closure. As a result, the ORR does not provide a clear or focused view of the most significant operational risks requiring organisational-level oversight, limiting management's ability to prioritise and respond effectively.
- **Weak risk escalation and siloed risk management:** HCPC does not have defined or consistently applied criteria for escalating risks from the ORR to the SRR. As a result, operational and strategic risks are managed largely in isolation, with limited visibility of how operational risk exposures contribute to strategic-level risk themes. No operational risks have been escalated in the past 12 months, increasing the risk that emerging or deteriorating issues are not brought to the attention of senior leadership or in a timely manner.
- **Key controls and mitigating actions:** Although HCPC identifies controls and mitigating actions within its risk registers, these are not clearly defined, consistently documented, or systematically monitored. Controls are often recorded at a high level or combined with future mitigation actions, making it difficult to distinguish what is currently in place versus what is planned. There is no structured process to assess control effectiveness, track progress of mitigating actions, or link controls to sources of assurance and a lack of a link with the risk appetite. This undermines confidence in residual risk ratings and limits assurance that risks are being managed within appetite.

Our testing did not identify any concerns surrounding the controls in place to mitigate the following risks:

- ✓ Roles and responsibilities for identification and management of risks are not clearly defined or understood, and or processes are overly reliant on single members of staff, which creates a lack of accountability or delays in the process.
- ✓ There is insufficient senior oversight of risks at HCPC and how these are being mitigated.
- ✓ Risk management is not considered in key strategic and business decision making and therefore decisions may be taken that are not aligned with the HCPC risk appetite.

Detailed Findings

Detailed Findings

Risks: Risks are not identified and reported through appropriate channels in a timely manner and escalated as required, leading to poor Board oversight and the inability to identify trend. Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risk.

Finding 1 - Absence of a mature ERM Framework	Type
In order for a risk management function to be effective, there should be a clear, documented and consistently applied approach to identifying, assessing, capturing, monitoring and escalating risks across the organisation. As part of our review of HCPC's approach to risk management, we assessed governance arrangements, risk identification and assessment processes, supporting documentation, and horizon-scanning activities across both strategic and operational risks. We identified that HCPC's risk management arrangements lack the consistency and maturity expected of an effective enterprise-wide framework. While aspects are operating in practice, such as responsibility for strategic and operational risks being clearly allocated to the Head of Assurance & Compliance and the Chief Information Security & Risk Officer respectively, the underlying processes have a number of weaknesses which reduce their overall effectiveness. • **Absence of a mature ERM Framework:** While HCPC has an Operational Risk Policy which serves as a ERM framework, the policy lacks key components expected of a comprehensive risk management framework. Specifically, it does not establish a unified, organisation-wide methodology for managing risks. There is also no equivalent policy or guidance for strategic risks, nor an overarching framework defining governance, roles, or a consistent approach to risk identification, assessment, mitigation, monitoring, escalation and closure. • **Risk identification and assessment:** Operational risks are identified and reviewed through quarterly discussions between the Chief Information Security & Risk Officer and directorate risk owners, while strategic risks rely on self-assessment and quarterly ELT discussions prior to review by ARAC. However, neither process is supported by a documented or standardised risk identification methodology or assessment template to be utilised in conjunction with aspects such as the scoring matrix. In addition, we identified instances where multiple strategic risks share identical risk ratings, mitigations and actions, reducing clarity over whether these risks are genuinely distinct or would be more effectively managed as a consolidated risk. Operational risks are also frequently raised verbally through ad-hoc prompt-based discussions (i.e "what keeps you up at night"), which while will help identify some risks, is inconsistent with the Operational Risk Management Policy requirement to identify risks through routine business activities and structured risk workshops to support more formalised capture of risks. • **Documentation and audit trail**: Quarterly operational risk meetings are not minuted, and there is no documented evidence of challenge, decisions or agreed actions. Similarly, ELT discussions informing updates to the SRR are not formally recorded. This limits traceability and increases reliance on individual knowledge rather than documented evidence. • **Horizon scanning:** While horizon scanning activity is undertaken through media, political and stakeholder monitoring, updates are largely dependent on quarterly discussions with limited formalised processes operating outside this cycle. In addition, sector and regulatory update communications do not consistently include the Risk Management team, reducing assurance that emerging risks are identified and escalated in a timely manner.	Design & Effectiveness 
Implication	**Significance**
The absence of a documented ERM Framework and structured risk management processes, supported by clear documentation reduces HCPC's ability to consistently and reliably identify, assess and escalate risks. In addition, the lack of documented meetings minutes and consistent horizon scanning increases the likelihood that significant risks may be overlooked or inaccurately prioritised, ultimately impairing effective risk-based decision-making.	Medium

Detailed Findings

Risks: Risks are not identified and reported through appropriate channels in a timely manner and escalated as required, leading to poor Board oversight and the inability to identify trends. Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risks.

Recommendations	Action owner	Management response	Completion date
1. HCPC should develop and implement a comprehensive and documented ERM Framework that establishes a consistent, organisation-wide approach to risk management for both Strategic and Operational risks and should include (above that which is already documented): • Purpose and scope • Governance structure (roles & responsibilities, committees, escalation routes) • Standard definitions (risk, control, appetite, tolerance) • Risk identification and assessment methodology (risk scores, ratings) • Control evaluation and assurance mapping requirements • Escalation thresholds between departmental → ORR → SRR • Reporting requirements and review cycles • Integration with strategy, planning, and performance • Training requirements In addition, HCPC should include in the framework: • Indicative limits or ranges for the number of risks within registers to ensure they remain manageable, supported by a supplementary reserve list for emerging risks not requiring full assessment • Clear criteria for risk closure (e.g. sustained control effectiveness, completion of treatment actions, or residual risk at or below target levels) • Clearly documented and consistently applied escalation criteria to ensure operational risks are escalated from the ORR to the SRR in a timely and proportionate manner.	*Anna Raftery, Head of Assurance and Compliance*	*We accept this recommendation.* *The Operational Risk Management policy and guide provides this detail for the approach to the ORR, however we do agree there is a gap in application and coverage. The Operational Risk Management policy will be reviewed and developed into a consistent and comprehensive ERM framework to cover the full organisational approach to risk.*	*31 March 2027* *[Q4 26-27 ARAC date]*

Detailed Findings

Risks: Risks are not identified and reported through appropriate channels in a timely manner and escalated as required, leading to poor Board oversight and the inability to identify trends. Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risks.

Recommendations	Action owner	Management response	Completion date
2. HCPC should introduce standardised templates for assessment of strategic and operational risks that work for all departments and utilise incident reporting, audit reports, audits and risk workshops to assess risks.	*Anna Raftery, Head of Assurance and Compliance* *[Vacant], Information Governance & Risk Lead*	*We accept this recommendation.* • *Risk assessments will be integrated into existing templates, and a standard template will be introduced for use as needed.* • *To assess risk, we will use existing reporting and audit and risk workshops.*	*30 June 2027* *[Q1 27-28 ARAC date]*
3. HCPC should formalise the documentation of all risk review meetings including quarterly meetings with risk owners and ELT, ensuring evidence of challenge, decisions and agreed actions are retained.	*Anna Raftery, Head of Assurance and Compliance*	*We accept this recommendation. We will use the AI transcription available in Teams to minute risk and assurance review meetings, if permission given by risk owner.*	*30 September 2026*
4. HCPC should ensure the existing horizon-scanning process include defined ownership and outputs from the process have clear escalation routes to risk management team.	*Anna Raftery, Head of Assurance and Compliance*	*We accept this recommendation. A&C will work with the Communications department to ensure there is a clear process for horizon-scanning escalation.*	*31 March 2027*

Detailed Findings

Risk: Risks are not identified and reported through appropriate channels in a timely manner and escalated as required, leading to poor Board oversight and the inability to identify trends. Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risk.

Finding 2 - Excess volume and data quality issues in the ORR	Type
An effective ORR should provide a clear and prioritised view of material operational risks, supported by clear risk articulation, defined controls, ownership of mitigating actions, alignment to risk appetite, and clear criteria for closing risks. As part of our review, we assessed the design and content of the ORR, including risk volumes, risk articulation, documentation of controls and actions, and data quality. We identified that the ORR contains an excessive volume of risks, reducing its effectiveness as a prioritisation and governance tool. At the time of review, the ORR contained 145 operational risks, which is materially higher than typically observed in comparable regulators and public-sector organisations. This suggests that operational risks are not being consistently assessed or managed at an appropriate level and is compounded by the absence of departmental or local risk registers to manage lower-level risks. Discussions with risk management indicated that the high volume of risks is partly driven by a cautious organisational culture and a perception among some risk owners that inclusion on the ORR may influence funding decisions. In addition, the ORR lacks defined criteria for closing or de-escalating risks, resulting in risks remaining on the register even where target risk levels have been achieved. For example, 48 of the 145 risks had residual risk ratings at or below their target risk ratings but had not been closed. ***(Please see Finding 1, Recommendation 1)*** Additionally, a review of ORR identified several gaps in how risks and controls are documented: ○ The risk descriptions in the ORR contain historical text, commentary, or project updates, rather than concise risk statements following a cause-event-impact structure. ○ The ORR contains multi-step scoring changes in inherent and post mitigation risks (e.g. 3 > 2 > 3) which complicates interpretation of residual risk ratings, although we note that this is an attempt to demonstrate changing risk levels over time. ○ A detailed review of the 145 risks in the ORR identified substantial data incomplete (Treatment steps / controls are explored in more detail in finding 4) across the 145 risks recorded: • 27 risks had no populated risk category (e.g., Public Protection, Finance, Reputation, Strategy) • Two risks had no “Treatment steps” • 107 treatment steps were marked as “Ongoing”, “TBC”, or “Unknown”, with some dates outdated (2022-2024), and 35 had no target date at all. • 11 “Treatment steps” had no assigned owner • 101 operational risks had no risk appetite categorised as minimal, open, measured or seeks as per scope area. As a result, the ORR in its current form does not consistently support effective prioritisation, clear accountability, or timely management of operational risks. This limits its usefulness as a management and governance tool and reduces assurance that operational risks are being actively managed and escalated.	Design & Effectiveness 

Detailed Findings

Risk: Risks are not identified and reported through appropriate channels in a timely manner and escalated as required, leading to poor Board oversight and the inability to identify trends. Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risks.

Implication	Significance
The high volume of risks and inconsistent quality of information make it difficult for senior management and Committees to readily identify, prioritise, and focus on the most significant operational risks requiring organisational-level oversight.	Medium

Recommendations	Action owner	Management response	Completion date
5. HCPC should undertake an immediate review of the ORR to confirm that risks recorded remain appropriate and if volume of the risks can be reduced. It should involve assessing if risks that have achieved their target residual rating can be formally closed or migrated to a departmental risk register, should these be implemented.	*Anna Raftery, Head of Assurance and Compliance* *[Vacant], Information Governance & Risk Lead*	*We accept this recommendation. The full review of the ORR will begin following the start of the new Information Governance & Risk Lead.*	*31 March 2027* *[Q4 ARAC date]*
6. HCPC should strengthen the quality of the ORR by: • Applying cause-event-impact risk statements and ensuring scoring is used consistently. Further, the risk team should resolve data quality issues by ensuring all risks have categories, treatment steps, owners, realistic target dates and defined risk appetite. • Ensure that risk appetite and target risk ratings in ORR are consistently documented for all operational risks and explicitly aligned to the agreed risk appetite framework. It should use these to assess if current and planned mitigations are sufficient to achieve the target risk and update as required. • Consider keeping a copy of ORR for internal consumption only. This copy should be used to document sensitive or IT - related controls that cannot be included in public-facing documents yet ensure they remain visible to those responsible for oversight.	*Anna Raftery, Head of Assurance and Compliance*	*We accept this recommendation. In the review and development of the new ORR we will ensure to include clear CEI risk statements and consistent data quality*	*31 March 2027* *[Q4 ARAC date]*

Detailed Findings

Risk: There is no clear governance structure in place for the escalation of risks between risk registers and the review of these risks by designated committees

Finding 3 - Weak risk escalation and siloed risk management	Type
An effective risk management framework ensures there is clear alignment between the SRR and ORR, with escalations from the ORR taking place where the risk has become significant enough. This ensures that those responsible for managing strategic risks have visibility of all risks which may impact the strategy, even where the risk was originally localised. Our review noted that there is no defined threshold for escalating operational risks to the SRR as per the Operational Risk Management Policy. As a result, no operational risks have been escalated to the SRR in the past 12 months, limiting the ability to identify when operational exposures may warrant strategic-level consideration. ***(Please see Finding 1, Recommendation 1)*** We also noted that the ORR and SRR operate largely in isolation, with limited visibility of how operational risks inform strategic-level themes. While not all high-scoring operational risks require escalation, the absence of documented linkage fields and clear escalation criteria restricts ARAC's ability to understand how operational exposures contribute to broader strategic risks across the organisation. Currently, ARAC undertakes an annual deep dive on a selected strategic risk and reviews the ORR once per year. Although operational risks were previously reported more frequently, ARAC indicated a preference for higher-level, strategic reporting, with an expectation that management would escalate risks as issues begin to deteriorate or concerns arise. However, in the absence of clear escalation mechanisms and systematic integration between the risk registers, this approach limits ARAC's and management's ability to maintain an organisation-wide view of its overall risk exposure.	Design & Effectiveness
Implication	**SIGNIFICANCE**
The absence of clear escalation mechanisms, combined with siloed risk management and high volume of risks in the ORR, undermines effective risk prioritisation and oversight. This increases the risk that emerging or deteriorating operational risks are not escalated, limiting ARAC's ability to maintain a clear view of the organisation's risk exposure.	Medium

Recommendations	Action owner	Management response	Completion date
7. HCPC should strengthen integration between the ORR and SRR by introducing clear linkage mechanisms that demonstrate how operational risks contribute to strategic-level risk themes.	*Anna Raftery, Head of Assurance and Compliance*	*We accept this recommendation* *There will be a clear mechanism to escalate operational Risks to the Strategic Risk Register, triggered if the inherent/current risk score hits 12.*	*31 March 2027*

Detailed Findings

Risk: Without determining and documenting key control activities in critical areas, management cannot identify the current level of mitigation, leaving vulnerabilities unaddressed and potentially resulting in significant incidents. Failure to monitor and adjust controls could result in ineffective measures, allowing fraud to occur and causing financial and reputational damage.

Finding 4 - Ineffective documentation and adjustment of key controls and future mitigating actions	Type
In order to gain assurance over risk management, organisations should clearly document key controls and future mitigating actions, demonstrate how these reduce inherent risk, and maintain a structured process for monitoring control effectiveness and delivery of mitigation plans. As part of our review, we assessed how key controls and mitigating actions are identified, documented, monitored and evidenced within the SRR and ORR. We identified that HCPC does not consistently or clearly document key controls or maintain assurance over whether controls are operating as intended. In addition, there is no structured process for monitoring control effectiveness or tracking the delivery and impact of future mitigating actions across either register. **SRR:** Within the SRR, controls are identified through management self-assessment and discussion rather than a clearly articulated or standardised risk assessment methodology. Controls are recorded at a high level as "mitigations in place", with limited detail on how they operate, their ownership, frequency, or how they reduce inherent risk to the assessed residual level and the same applies to planned future actions. While target risk levels are recorded, there is limited evidence of how controls and planned actions are monitored for implementation to confirm that strategic risks are being actively managed within appetite or whether further mitigation is required. **ORR:** Within the ORR, "Treatment Steps" are used in place of clearly defined key controls and often combine existing controls with future or incomplete actions, making it difficult to distinguish what is currently operating, and these again lack sufficient detail on aspects such as how they operate, their ownership, frequency, or how they reduce inherent risk to the assessed residual level, although we note the ORR lacks this detail due to it being a public facing document. We also noted issues with the link between controls, risks and risk appetite, with 31 risks having no movement from the inherent risk score despite controls being listed, 101 risks not having a risk appetite defined, 27 risks not having a target risks and 42 risks with residual risk above target, but no future mitigations listed. This inconsistency means management cannot reliably assess whether current controls are sufficient or whether risks that remain above appetite are being actively mitigated. ***(Please see Finding 2, Recommendation 6)*** Finally, assurance over controls in both the SRR and ORR relies heavily on management declarations, often provided verbally, with limited linkage to supporting evidence. This reduces confidence in residual risk ratings and limits assurance that risks are being managed in line with HCPC's agreed risk appetite.	Design & Effectiveness 
Implication	**Significance**
Without clearly defined, consistently documented, and independently validated key controls, supported by target risk aligned to risk appetite, management is unable to reliably determine whether controls are operating as intended or whether risks are being effectively mitigated. This undermines the credibility of residual risk ratings and increases the likelihood that significant weaknesses remain undetected and unaddressed.	Medium

Detailed Findings

Risk: Without determining and documenting key control activities in critical areas, management cannot identify the current level of mitigation, leaving vulnerabilities unaddressed and potentially resulting in significant incidents. Failure to monitor and adjust controls could result in ineffective measures, allowing fraud to occur and causing financial and reputational damage.

Recommendations	Action owner	Management response	Completion date
8. For the SRR and ORR HCPC should: • Clearly document and separate "key controls" or "mitigations in place/ treatment steps" and "proposed/future mitigating actions"— including a detailed control description, purpose, control type (preventive/detective), ownership and frequency of control. • Move its approach to identifying key controls by analysing the causes and consequences of risks, for example by using Bow-Tie analysis. Bow-Tie analysis is a structured risk assessment and visualisation technique used to understand, analyse, and manage risks by clearly mapping the relationship between the threats that could cause a risk event, the risk event itself (often referred to as the "top event"), and the potential consequences that may arise if the event occurs. • Establish a formal process for recording, monitoring, and updating future mitigating actions/ treatment steps. This process should ensure that each action has an assigned owner, realistic target date, and a regular progress review. • Link its existing assurance sources to each key control to validate that controls are operating as intended, which is an evolution from its existing assurance mapping. This should include referencing evidence such as Council papers, Internal Audit reports, project completion documentation, Professional Standards Authority reports, and other relevant assurance outputs and support alignment with Provision 29.	*Anna Raftery, Head of Assurance and Compliance*	*We accept this recommendation.* *In the new risk framework, the SRR and ORR will be managed clearly, consistently and proportionately. We will investigate the best way to appropriately evidence controls and future actions/mitigations using existing documentation. However, it is unrealistic to require documented evidence for all operation risk mitigations across 12 areas on a quarterly basis. The appropriate resource is not available for this level of scrutiny.*	*31 March 2027* *[Q4 ARAC date]*

Observations

Operational Risk Management Policy
We noted that the annual review of the ORR by the ARAC is not referenced within the HCPC Operational Risk Management Policy v1.1. While the Policy states that it should be reviewed and updated following a significant business change, the planned review of the Corporate Strategy and risk appetite in 2026 presents an opportunity to update the Policy. This update would allow HCPC to formally document governance arrangements, including ARAC's role in overseeing and reviewing the ORR, and ensure the Policy remains aligned with current risk management practices.

Appendices

Appendix I: Risk Register Layout - Template

Below we have included an example header layout of a good practice risk register. by laying out risk registers in this way, individuals can easily understand the flow of risk management from inherent to residual (left to right) with controls, risk appetite, and appropriate actions all in one place. this should help with clarity, reducing siloed working, and help to trim down the ORR.

Risk ID	Process	Risk Description	Causes & Consequences	Risk Owner	Risk Likelihood (1 - 5)	Risk Impact (1- 5)	Inherent Risk Score	Key or Current Mitigating Controls	Risk Likelihood (1 - 5)	Risk Impact (1 - 5)	Residual Risk Score	Source of Assurance	Risk Appetite or Target Risk	In Appetite? (Y/N)	Future Action Plan	Action Owner	Target Date	Risk Movement

Appendix II: Definitions

Level of assurance	Design of internal control framework		Operational effectiveness of controls	
	Findings from review	Design opinion	Findings from review	Effectiveness opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

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

Appendix III: Terms of Reference

Extract from terms of reference		
Purpose		
The purpose of the review was to provide assurance over the control design and effectiveness of key risk management controls in operation at HCPC.		
Scope area	**Key risks**	**Approach**
• Risk identification assessment and mitigation	• Risks are not identified and reported through appropriate channels in a timely manner and escalated as required, leading to poor Board oversight and the inability to identify trends. • Without determining and documenting key control activities in critical areas, management cannot identify the current level of mitigation, leaving vulnerabilities unaddressed and potentially resulting in significant incidents. • Failure to monitor and adjust controls could result in ineffective measures, allowing fraud to occur and causing financial and reputational damage.	• We will assess how management has identified its keys risk (such as through risks assessments), including assigning owners, assessed inherent and target risk ratings and how often these are re-assessed. This will include any horizon scanning performed of sector/regulatory risk, ensuring there are sufficient inputs into the assessment and that appropriate expertise has been used to support development. • Test a sample of completed risk assessments to assess if the correct process was followed and how the actions from the assessment have been/ are being implemented. We will also assess the last time these were reviewed to check they are up to date. • We will assess how management determines what risks should be included in the strategic or operational risk register, including any processes for escalation, and how it prioritises risks, so registers are not overburdened with a significant number of risks compared to good practice. • We will review the risk registers and identify any clear gaps and benchmark the volume of risks included against similar organisations. • We will assess how management determines the controls it has in place to mitigate risks and the level of mitigation this brings to the inherent risk level. We will also understand how management identifies the actions to take to further mitigate the risk to the target level and if these are assigned owners and due dates. As part of our review, we will assess if these are clearly distinguished in the risk registers. • We will select a sample of risks and assess if the actions have been assigned owners and due dates and if these are regularly reviewed and updated (for example, no historical dates). • We will assess how management reviews the effectiveness of the controls it has put in place to mitigate risk and as part of this we will consider how management makes any changes to controls in respect to these reviews.

Appendix III: Terms of Reference

Extract from terms of reference		
Scope area	**Key risks**	**Approach**
• Risk appetite	• Management is unaware of its appetite and tolerance for risk and thus under or over controls its key risks, leading to inefficient use of resource.	• We will assess if management has a risk appetite in place and how often this is re-assessed. We will also understand how it is applied in practice when determining target risk ratings. • For a sample of risks, we will understand how management determined the target risk rating to apply and if this appears aligned with the risk appetite. (benchmark- risk register)
• Policies, procedures, framework and guidance	• Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risks. • Roles and responsibilities for identification and management of risks are not clearly defined or understood, and or processes are overly reliant on single members of staff, which creates a lack of accountability or delays in the process.	• We will review the risk management policies and procedures and assess whether roles and responsibilities in relation to risk management have been clearly defined, communicated to staff and are being applied in practice. This will include whether staff have received appropriate guidance, support and training in relation to risk identification and management, and whether they are kept up to date as changes to processes /requirements are made. We will also assess if the process is robust enough to avoid bottlenecks. • We will assess if the policies and procedures are accessible and communicated effectively.
• Governance and reporting	• There is no clear governance structure in place for the escalation of risks between risk registers and the review of these risks by designated committees. • There is insufficient senior oversight of risks at HCPC and how these are being mitigated. • Risk management is not considered in key strategic and business decision making and therefore decisions may be taken that are not aligned with the HCPC risk appetite.	• We will review the risk management governance structure in place, including how risk registers feed into each other and the committees that are responsible for the risk registers. We will understand how often reports are made to these committees, what content is included in these and assess if this is sufficient to provide appropriate oversight and enable informed decision making • We will select a sample of reporting periods and assess if the reports have been produced and provided to the relevant committees. • We will interview staff to understand how risk is considered when making key business decisions, such as in relation to the strategy, business cases or project management. We would support this by review of documents that evidence risk being a part of the decision-making process, such as project management methodologies, the corporate plan and recent business cases. - • Review a sample of ELT papers to assess how risk management has been considered in strategic decision making.

Appendix III: Terms of Reference

Extract from terms of reference		
Scope area	**Key risks**	**Approach**
• Risk appetite	• Management is unaware of its appetite and tolerance for risk and thus under or over controls its key risks, leading to inefficient use of resource.	• We will assess if management has a risk appetite in place and how often this is re-assessed. We will also understand how it is applied in practice when determining target risk ratings. • For a sample of risks, we will understand how management determined the target risk rating to apply and if this appears aligned with the risk appetite. (benchmark- risk register)
• Policies, procedures, framework and guidance	• Policies and procedures are poorly designed, not accessible and do not support identification, escalation, documentation and mitigation of risks. • Roles and responsibilities for identification and management of risks are not clearly defined or understood, and or processes are overly reliant on single members of staff, which creates a lack of accountability or delays in the process.	• We will review the risk management policies and procedures and assess whether roles and responsibilities in relation to risk management have been clearly defined, communicated to staff and are being applied in practice. This will include whether staff have received appropriate guidance, support and training in relation to risk identification and management, and whether they are kept up to date as changes to processes /requirements are made. We will also assess if the process is robust enough to avoid bottlenecks. • We will assess if the policies and procedures are accessible and communicated effectively.

Extract from terms of reference
Exclusions/ limitations of scope
The scope of the review is limited to the areas documented under the scope and approach detailed overleaf. All other areas are considered outside of the scope of this review. Specifically, we are not: ▶ Assessing the assurance mapping process ▶ Undertaking a detailed review of the mitigating controls in place, only that they have been identified, documented and assessed. ▶ Confirming if the risks identified and reported are the most appropriate. Our work is inherently limited by sampling risks and therefore will not provide assurance over all processes. We are reliant on the honest representation by staff and timely provision of information as part of this review.

Appendix IV: Staff Interviewed

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.		
Anna Raftery	Head of Assurance and Compliance	Key contact
Roy Dunn	Chief Information Security & Risk Officer	Key contact
Nicole Jones	Improvement & Compliance Specialist	Key contact

Appendix V: Limitations and Responsibilities

Management Responsibilities

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

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

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

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

Limitations

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

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

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

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

Conformance with the Global Internal Audit Standards

This engagement has been conducted in accordance with the Institute of Internal Auditors' Global Internal Audit Standards.

FOR MORE INFORMATION:

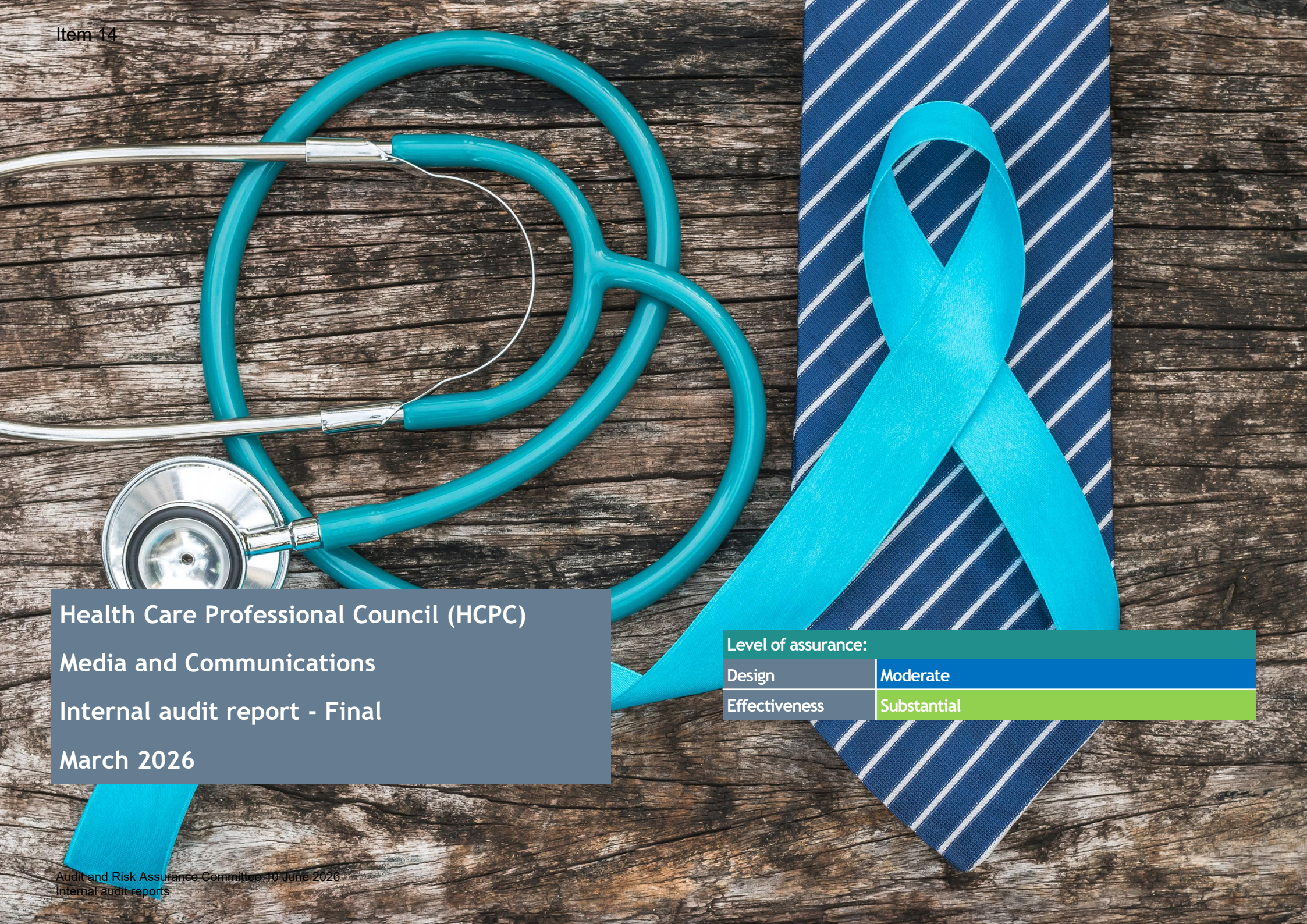
Bill Mitchell, Director

Bill.Mitchell@bdo.co.uk

Sarah Hillary, Partner
Sarah.Hillary@bdo.co.uk

www.bdo.co.uk

42001482



Health Care Professional Council (HCPC)

Media and Communications

Internal audit report - Final

March 2026

Level of assurance:	
Design	Moderate
Effectiveness	Substantial

Contents

Restrictions of use

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

Distribution list		
For action	Matthew Peck	Head of Communications and Engagement
	Lisa Greenhill	Communications Strategy Lead
	Tony Glazier	Digital Communications Content Lead
For information	Anna Raftery	Head of Assurance and Compliance
	Audit Committee	

Report status	
Auditor:	Shamail Afroz, Senior Auditor
Reviewers:	Bill Mitchell, Director
Dates work performed:	5 December 2025 to 13 February 2026
Closing meeting:	13 February 2026
Additional documents and queries:	N/A
Draft report issued:	6 March 2026
Management responses received:	12 March 2026 and 30 March 2026
Final report issued:	30 March 2026

Executive summary

Level of assurance: (see appendix I for definitions)		
Design	Moderate	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	Substantial	The controls that are in place are being consistently applied.

Definitions of findings (see appendix I)		# Of agreed actions
H	0	0
M	1	3
L	0	0
Total number of findings: 1		

Purpose

The purpose of the review was to provide assurance over the control design and effectiveness of key media and communications controls in operation at HCPC.

Background

As part of the agreed internal audit plan for 2025/26, as approved by the Audit and Risk Assurance Committee (ARAC), we have undertaken a review of key controls in respect of media and communications. HCPC has been on a journey with respect to its approach to media and communications over the last few years. Historically, HCPC has largely used an external provider to support the communications function and while a small internal team was in place; their primary focus was on maintaining digital channels and transactional publication of updates.

More recently, since the appointment of the new Head of Communications and Engagement, HCPC has been aiming to bring more communications activity in-house, by building on the skills that are already in the team and actively recruiting to fill any skills and capability gaps.

A Communications Strategy was agreed in July 2024, the aim of which is to put in place the building blocks for a high performing communications function, improved communications capability across the organisation and a stronger HCPC brand. The Strategy sets out a more ambitious and confident approach to communications, reflecting HCPC's "open" risk appetite in this area and a desire to be more visible, influential, and consistent in its messaging.

Over the last 18 months, progress has been made against the Strategy, with the most recent update (July 2025) confirming that 78% of strategic activity measures were completed or in progress. This has mainly involved re-building the in-house team and redesigning processes. This focused first on the Digital and Strategic Communication teams. Most recently the media capability in the team was enhanced by the appointment of a Media Officer and Internal Communications Manager.

The Communications Strategy highlighted the need for clearer planning, commissioning and coordination, and this work is now underway through the Corporate Affairs Workplan for communications and engagement and a Communications Grid.

As the in-house capacity has been growing the external provider has continued to provide support, but with a reduced remit and budget. A key focus for management is on ensuring that controls are appropriate and balance the need for agility when required, with the need to manage risk in a proportionate manner.

HCPC has also enhanced its data-driven oversight through the Comms Live Dashboard, which tracks key indicators such as website traffic, social media performance, hub usage, media mentions, etc.

Our testing did not identify any concerns surrounding the controls in place to mitigate the following risks:

- ✓ There is no plan in place to ensure the Communication Strategy can be delivered, such as through the provision of sufficient resource.
- ✓ HCPC has no clear approach to communications resulting in inadequate and disjointed communications to its stakeholders
- ✓ Potential stakeholders have not been identified and targeted through communication activities.
- ✓ HCPC's approach to Communications fails to ensure compliance with good practice.
- ✓ Roles and responsibilities have not been clearly defined or understood, resulting in duplication of activity or an absence of accountability
- ✓ Proactive and reactive communications are undertaken which are not authorised or accurate, in line with policies and procedures (i.e. established style guides) or sent to the wrong individuals or organisations, which could result in negative public exposure.
- ✓ Management is not aware of the effectiveness and performance of communication activities leading to an inability to take remedial actions to address inefficiencies and poor performance

Executive summary

Summary of good practice

- A Communications Strategy (2024-26) is in place which is regularly reviewed and reported against to the Council annually. The most recent update (July 2025) confirmed that 78% of strategic activity measures were either completed or in progress, evidencing proactive delivery and continuous monitoring of progress.
- The Corporate Affairs Workplan reflects clear alignment between communications strategy and corporate strategic aims, with clear project or capability building deliverables and timelines.
- Roles and responsibilities within the Communications team are clearly established through job descriptions and the communications planning process. A business case presented to the Executive Leadership team (ELT) and approved by the Executive Director introduced new roles to strengthen in-house capability through a three phased approach.
- A structured communications planning process is in place, ensuring all new work is commissioned through a standardised form, assessed at a weekly planning meeting and progressed through clear stages including planning, delivery, approval and evaluation.
- The Media and Political Interest Escalation Policy provides strong controls for managing high-risk and sensitive external communications, with clearly defined responsibilities across Luther Pendragon (external provider), the in-house Communications team, ELT, the CEO and the Chair. This will be further updated as they transition to a more in-house approach.
- A six months Communications Grid is in place which maps organisational announcements, internal messaging, stakeholder engagement, hearings, FOI (Freedom of information) and renewal cycles across short and long-term horizons.
- A Comms Live Dashboard provides data-driven oversight of communications performance. The dashboard tracks key indicators such as website activity, social media engagement, hub usage (student, employer, data and sexual safety hubs), media mentions, inbound queries, and performance of priority campaigns.
- Sample testing of both proactive and reactive communications, including time-sensitive and Fitness to Practise (FtP) enquiries, confirmed that all communications follow the required approval routes via the Head of Communications, the Deputy Chief Executive & Executive Director of Education, Registration & Regulatory Standards, or the Executive Director of Fitness to Practise and Tribunal Services where relevant.

Useful statistics and key takeaways

189K
Website users as of November 2025

164k
Social media followers as of September 2025 including LinkedIn with highest (56%)

43
Media mentions in November 2025, as per the monthly ELT Communications Grid

5
Proactive media communications such as press release or broadcast were completed in a year as of October 2025

Area for improvement

However, we have identified one findings of Medium significance:

Risk Assessment: While HCPC's 2024-2026 Communications Strategy adopts an "Influence and Leadership" risk appetite, external communications risks—including media handling—are currently assessed through informal judgment-based processes rather than a documented and consistently applied risk assessment framework. Decisions on how to engage with media, MPs, sector stakeholders or sensitive issues are therefore made on a case-by-case basis without an evaluation of reputational, operational or regulatory risks against an evaluation matrix.

Conclusion

HCPC has developed and implemented a structured and well-coordinated approach to managing its communications and media activity, supported by detailed processes and a live dashboard which provides robust data insight across core communications channels.

Detailed findings

Detailed findings

Risk 6: The process for various types of proactive and reactive communications via various channels is inefficient, or control is too weak, based on the controls not being aligned to the risk appetite

Finding 1 – Risk assessment	Type
Effective external and media communications should be supported by an organisation's clearly defined, consistently applied risk assessment framework. The approach enables the organisation to identify, evaluate and document reputational, regulatory, operational and stakeholder-related risks, ensuring that communication decisions are aligned to the organisation's risk appetite and supported by an appropriate document trail. HCPC does not currently have a formal, consistently applied mechanism for identifying, assessing, and responding to risks associated with external and media communications that enables the organisation to be aligned to its risk appetite. HCPC adopted a proactive "Influence/Leadership - Seeks" risk appetite as part of it's 2024-2026 Communications Strategy, which translates into willingness to take decisions which are likely to bring additional scrutiny of the organisation. Discussion with management during our review confirmed that the assessment of external and media communications risks relies on professional judgement rather than a documented and consistently applied framework. As a result, decisions relating to media and external communications are made on a case-by-case basis supported by subject matter experts, media specialists within the team, and consultation with senior management. During our review, sample testing of three proactive communications identified that in two cases, risks were discussed informally (e.g. planning meetings or other conversations regarding the case) with limited documented evidence demonstrating how risks were assessed or mitigated. In one case, risks were formally documented within a Communication plan, including associated mitigation actions. In addition, sample testing of three reactive communications (all relating to Fitness to Practise enquiries) noted that senior stakeholders — such as the Deputy Chief Executive & Executive Director of Education, Registration & Regulatory Standards, the Executive Director of Fitness to Practise and Tribunal Services, and the Head of Communications — were involved in reviewing responses. However, risk considerations were not explicitly articulated or documented within the inquiry tracker or supporting email correspondence, although we note management's view is this would potentially increase risk exposure if too much detail was documented. We noted that a "Media and Political Interest Escalation Policy" is in place which outlines the approval pathway for media commentary. However, this policy does not include a structured risk assessment methodology or legal review matrix applicable across all communication types. Additionally, the recently introduced "Press Office Protocol 2025" sets out sign-off requirements based on perceived risk levels (high, medium, low) but does not define the criteria for determining or assessing these risk categories. While multiple staff members are involved in this process, the risk assessment of proactive and reactive remains largely dependent on individual judgement and experience. Whilst we acknowledge implementing a highly prescriptive framework may not align with an open or proactive risk appetite; the absence of minimum guiding principles for risk assessment results in inconsistent documentation and limited audit trail.	Design 

Detailed findings

Risk 6: The process for various types of proactive and reactive communications via various channels is inefficient, or control is too weak, based on the controls not being aligned to the risk appetite

Implication	Significance
Lack of defined and documented risk assessment for proactive and reactive media communications may increase the risk of inconsistent decision-making, insufficient senior oversight and limited audit trail for media and communications, exposing HCPC to scrutiny and potential reputational harm, particularly in cases involving high-profile or sensitive enquiries.	Medium

Recommendations	Action owner	Management response	Completion date
1. HCPC should update the 'Press office Protocols 2025' to include a 'Crisis Communications Manual' that outlines a formal, simple, consistently applied risk assessment framework for all external and media communications. This should include: • Definition of minimum risk assessment criteria (e.g. reputational, legal, regulatory, stakeholder impact). • Clear definitions for distinguishing high, medium and low-risk communications and risk mitigation process, aligned to HCPC's stated risk appetite. • The framework should recognise that cases tend to be fast moving and processes needs to be flexible and fit for purpose so that individuals and teams are empowered to act. This could include ensuring there is a designated individual who can approve communications outside of the normal approval route if there is a increased risk of not responding in a timely manner. These decisions should be sense checked in line with the regular review of decisions taken. 2. The team should capture the rationale for risk ratings, key considerations, and approvals within communications planning documentation and the inquiry tracker, relating to proactive and reactive communications. These should only be high-level and short written descriptions. 3. The Media and Comms team should introduce a quarterly review process to analyse any proactive or reactive communications where a formal risk assessment may not have been completed, retrospectively assess the level of risk involved (e.g., reputational, operational, regulatory, stakeholder impact), and document any lessons learned, feeding them into continuous improvement activities such as updates to the Press Office Protocols, team training and communications planning processes.	Matthew Peck, Head of Communications and Engagement	1. We accept the recommendation. We already have plans in place to develop a crisis communications manual that will include a risk matrix. While a risk framework may enhance our ability to induct new members of staff, help clarify expectations on decision making with internal stakeholders and help explain our decision making retrospectively, it is unlikely to be of use in day to day operations due to the fast paced nature of media activity and the nuance of each individual inquiry/issue. A too prescriptive approach may in fact limit our ability to meet our risk appetite in this area by adding bureaucracy. 2. We accept this recommendation. We will seek to capture additional information to that already captured in our documentation of proactive and reactive communications. 3. We accept this recommendation. We will implement a quarterly review process to identify learning.	31 January 2027

Observations

Delay in escalating time-sensitive media enquiries

Our review of three urgent media or negative communications handled in the last twelve months identified one case where a time-critical enquiry was not escalated promptly to the Communications team. Specifically, a journalist from BBC Yorkshire Online contacted the Information inbox on 16 December 2025 seeking clarification regarding a suspension order to support accurate reporting. The enquiry was forwarded to the Hearing Team Managers on 17 December 2025 and subsequently routed to the press inbox later the same day. Due to the delay in escalation, HCPC did not provide a response before the journalist's publication deadline, and the story was released without HCPC comment. The Media Communications Officer later issued an apology to the journalist.

This demonstrates that delays in forwarding urgent media enquiries can result in missed opportunities to provide accurate context, potentially resulting in negative or unbalanced reporting. We noted that HCPC has planned an internally led media session with the TST team to reinforce new processes and expectations for handling journalist approaches. In addition, HCPC's website clearly instructs external parties to direct media enquiries to the Communications team.

Appendices

Appendix I: Definitions

Level of assurance	Design of internal control framework		Operational effectiveness of controls	
	Findings from audit	Design opinion	Findings from audit	Effectiveness opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

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

Appendix II: Terms of reference

Extract from terms of reference		
Purpose		
The purpose of the review was to provide assurance over the control design and effectiveness of key media and communications controls in operation at HCPC.		
Scope area	**Key risks**	**Approach**
Communications Strategy	There is no plan in place to ensure the Communication Strategy can be delivered, such as through the provision of sufficient resource. HCPC has no clear approach to communications resulting in inadequate and disjointed communications to its stakeholders. Potential stakeholders have not been identified and targeted through communication activities. HCPC's approach to Communications fails to ensure compliance with good practice. Roles and responsibilities have not been clearly defined or understood, resulting in duplication of activity or an absence of accountability	• We will assess the adequacy of HCPC's Communication Strategy including: • The completeness of content within the Communications Strategy against recognised good practice. • The process for producing, reviewing, approving and communicating the Communications Strategy to relevant stakeholders (internal and external). • Whether stakeholder mapping has been completed that identifies key stakeholders, their needs and the frequency of communication, including approaches to engage with stakeholders that are either not currently being communicated with or are not being engaged with to the desired level. • Steps taken to ensure the delivery of the communications strategy, including any operational plans, action plans, and resources allocated. Where applicable we will also assess whether key milestones have been identified and plans to achieve these have been documented. • Whether the Communications Strategy aligns with the Corporate Strategy. • Assess HCPC's compliance with key aspects of good practice. • Assess whether roles and responsibilities of the Communications team (and any other relevant staff) have been clearly assigned and have been documented within the Communications Strategy and any relevant policies and procedures. Consideration will be given to whether there are any gaps in ownership and whether there is sufficient resource to deliver the Strategy in the event of HCPC needing to respond to significant amount of external events.
Communications and risk appetite	The process for various types of proactive and reactive communications via various channels is inefficient, or control is too weak.	• We will assess how management determines the controls to put in place dependent on the level of risk involved and aligning this to the appetite, to ensure controls are both effective but efficient. • Review policies, procedures and guidance documents to assess control design and completeness of process documentation. This will include how content is created, reviewed and authorised before being posted/issued and whether there are any style guides.

Appendix II: Terms of reference

Extract from terms of reference		
Scope area	**Key risks**	**Approach**
Communications and risk appetite	Proactive and reactive communications are undertaken which are not authorised or accurate, in line with policies and procedures (i.e. established style guides) or sent to the wrong individuals or organisations, which could result in negative public exposure.	• Review the Communication Strategy and relevant policies and procedures to identify and assess the processes in place to react and respond to unexpected negative press and/or external events that require external communications to be produced in a short period of time without compromising the day-to-day activity of the Communications team. • Select a sample of communications and assess if these were appropriately approved and sent to the correct groups and individuals.
Management information	Management is not aware of the effectiveness and performance of communication activities leading to an inability to take remedial actions to address inefficiencies and poor performance.	• Evaluate the mechanisms HCPC have in place to review the effectiveness of communication and campaigns used by HCPC. This will include any lessons learned, corrective action taken, and the content and frequency of reports produced for management.

Appendix II: Terms of reference

Extract from terms of reference
Exclusions/ limitations of scope
The scope of the review is limited to the areas documented under the scope and approach detailed overleaf. All other areas are considered outside of the scope of this review. Specifically, we are not: • Providing detailed assurance about the content of the Communication Strategy, only that it considers the fundamentals to set it up for success, such as having the appropriate resource. • Assessing if the content of communications are accurate, only that there are processes in place to support this. Our work is inherently limited by sampling risks and therefore will not provide assurance over all processes. We are reliant on the honest representation

Appendix III: Staff interviewed

We appreciate the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.		
Matthew Peck	Head of Communications and Engagement	Action owner
Lisa Greenhill	Communications Strategy Lead	Interviewee
Tony Glazier	Digital Communications Content Lead	Interviewee
Nicole Jones	Improvement & Compliance Specialist	Key contact

Appendix IV: Limitations and responsibilities

Management responsibilities

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

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

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

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

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

Limitations

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

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

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

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

Conformance with the Global Internal Audit Standards

This engagement has been conducted in accordance with the Institute of Internal Auditors' Global Internal Audit Standards.

For more information:

Bill Mitchell, Director

Bill.Mitchell@bdo.co.uk

www.bdo.co.uk

00412624