Audit and Risk Assurance Committee

Meeting Date	18 September 2025
Title	Operational risk register annual review
Author(s)	Roy Dunn, Chief Information Security and Risk Officer
Executive Sponsor	Claire Amor, Executive Director of Corporate Affairs

Executive Summary

This paper presents the annual review of the operational risk register (ORR) for the period August 2024 to August 2025. The ORR is a key tool for identifying, assessing, and managing operational risks across the HCPC. It is reviewed quarterly by risk owners and annually by the Audit and Risk Assurance Committee to ensure continued relevance and alignment with organisational priorities. Mitigations apply to risks when fully implemented.

This year's review highlights several developments:

- Risk profile evolution: The total number of risks has increased slightly, with a notable shift toward higher residual risk scores. This reflects both external pressures and internal changes, including regulatory reform, cyber threats, and workforce challenges.
- Key influences: Organisational stability has improved following changes to the Executive Leadership Team ELT) and the implementation of a fee increase. However, financial constraints, supplier reliability, and ongoing cyber incidents continue to shape the risk landscape.
- Emerging risks: New risks have been identified in areas such as artificial intelligence (AI) adoption, data privacy, and partner contract changes. These reflect evolving operational realities and the need for proactive mitigation strategies.
- Directorate-level insights: The review provides a detailed breakdown of risks across directorates, highlighting areas of concern and improvement. Notable updates include strengthened governance processes, increased resourcing for feedback and complaints, and enhanced risk management in education and registration.

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

Previous consideration	The summary was reviewed by the ELT prior to circulation to the Committee.
Next steps	Operational risks will continue to be monitored and updated on a quarterly basis.
Financial and resource implications	None predicted
Associated strategic priority/priorities	Relevant to all strategic priorities.
Associated strategic risk(s)	Relevant to all strategic risks
Risk appetite	Compliance - measured
Communication and engagement	None
Equality, diversity and inclusion (EDI) impact and Welsh language standards	None
Other impact assessments	None
Reason for consideration in the private session of the meeting (if applicable)	Not applicable

Operational Risk Register Annual Review

1. Introduction

1.1 The operational risk register (ORR) is reviewed and updated on a quarterly basis through structured meetings with risk owners across the organisation. These updates typically reflect incremental changes to inherent and residual risk levels, often driven by shifts in resourcing or the completion of projects that introduce new capabilities.

1.2 Approaches to risk review vary across departments. Some undertake a comprehensive reassessment of their risks, effectively starting from a blank slate. Others adopt a more iterative, continuous improvement approach, updating their risks as part of ongoing operational activity. Mitigations are considered operational when they are in place. Planned mitigations do not lower current risk levels.

1.3 To maintain focus and brevity, this paper does not explore all areas in equal depth. Instead, it highlights those areas deemed to be of particular relevance or concern to the Committee.

1.4 This report covers the period August 2024 to August 2025.

2. High level influences on the operational risk register.

2.1 Following the changes to the Executive Leadership Team (ELT) in the previous reporting period, the team has remained largely stable. One member was on maternity leave and returned to full-time duties towards the end of 2024. The management team is experienced and well-versed in working with both the Council and its Committees.

2.2 A fee increase has been implemented, generating additional income as professional renewals progress. Further fee adjustments are under consideration to support long-term financial sustainability. While the organisation continues to operate within tight financial constraints, its short to medium term outlook has improved.

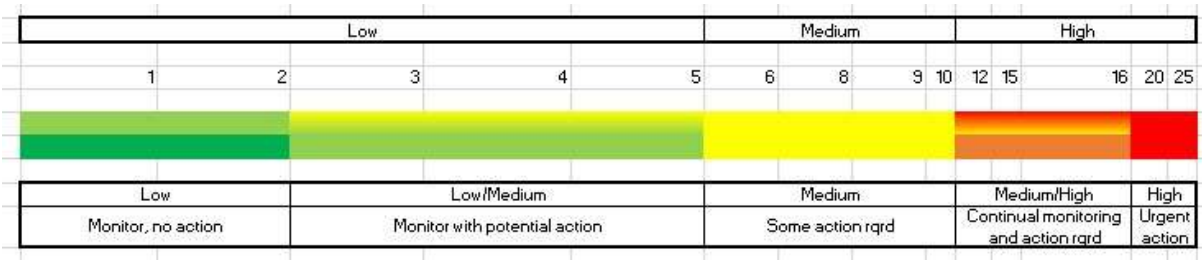
2.3 Regulatory reform has seen limited progress over the past year due to reasons outside of the HCPC's control. The government has linked the HCPC's reform to the regulation of hospital managers, reaffirming its commitment to modernising the legislative framework within this parliamentary term. Efforts are ongoing to ensure alignment between these reform initiatives.

2.4 Organisational confidence is growing, supported by the now meeting 17 of the 18 standards of the Professional Standards Authority (PSA). However, this progress remains dependent on not being complacent, continuous improvement and active monitoring of our performance and that of our suppliers.

2.5 A continuing cyber-attack involving SMS toll fraud by external actors has resulted in increased costs. The organisation is seeking reimbursement of excess costs from Microsoft and has now transitioned away from SMS-based user authentication. The new approach utilises the Microsoft Authenticator app or email-based authentication. Microsoft has already restricted SMS authentication in certain countries, ahead of the organisation's full implementation of the new solution. Note: this change to the authentication process was complete on 10 September 2025.

3. Overview of current and past levels of operational risks

3.1 Levels of risk currently use the following score matrix:



Catastrophic	5	10	15	20	25
Significant	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5
	Highly Unlikely	Unlikely	Possible	Likely	Highly Likely

3.2 Overview of current and past levels of operational risks:

	Low 1-2	**Low/ Medium 3-5**	**Medium 6-10**	**Medium / High 11-15**	**High 16-25**	Total Risks
Total Risks 2023	5	31	88	20	0	144
Total Risks 2024	4	27	85	22	6	144
Total Risks 2025	2	29	80	25	6	142

3.3 The table below presents the number of operational risks recorded within each department, comparing scores from August 2024 and August 2025. These are shown as ratios (e.g. 5/3) to indicate the change over time. Efforts have been made to consolidate common risks—either by merging them under Senior Leadership Team (SLT) ownership or removing them where they are no longer considered significant.

3.4 All operational risks are owned by Senior Leadership Team members.

Department - August 2024 vs. 2025	Low 1-2	Low/ Medium 3-5	Medium 6-10	Medium / High 11-15	High 16-25
Corporate Affairs					
Chair & CEO Office (previously listed with Governance)	0/0	-/2	-/1	0/0	0/0
Information Governance & Security	0/0	2/2	8/9	3/6	0/0
Feedback & Complaints	0/0	0/0	0/2	0/1	1/0
Quality Assurance	0/0	0/0	4/3	2/0	0/0
Governance	0/0	0/1	7/6	0/0	0/0
Partners	0/0	0/0	5/5	1/1	2/2
Communication	0/0	1/2	8/6	0/0	0/0
Strategic Relationships	0/0	1/1	4/4	0/0	0/0
Professionalism, and Upstream Regulation	0/0	1/1	0/0	0/0	1/1
Education, Registration and Regulatory Standards					
Education	0/0	7/7	7/7	0/0	0/0
Insight and Analytics	0/0	0/0	2/1	1/2	0/0
Policy and Standards & EDI	0/0	1/3	5/3	2/2	0/0
Registration & CPD	0/0	1/0	3/5	5/2	1/0
Regulation Development & Performance (new)	-/0	-/0	-/2	-/0	-/0
Fitness to Practise & Tribunal Service					
Fitness to Practise	0/0	0/0	6/6	2/6	1/2
Resources					
Estates & Facilities	0/0	2/2	6/6	0/0	0/0
Finance & Procurement	1/1	5/4	4/4	1/0	0/0
Information Technology	0/0	0/0	6/4	1/1	0/1
Human Resources	0/0	2/0	5/2	0/3	0/0
Business Change	3/1	5/6	6/3	0/0	0/0
ELT now listed under SLT	0/0	1/0	7/3	4/4	0/0
TOTAL RISKS	4/2	27/29	85/81	22/30	6/6

3.5 The residual risks remaining at High are as follows:

Trained resource attrition impacts operations [FTP14; IR16/RR16]	Attrition of fitness to practise (FTP) employees, results in potential delays to cases as, the notice period is shorter than the recruitment period, and ready skilled replacements are not available, causing a lack of resilience even with inhouse training to cover technical shortfalls.
Inaccurate public Register [FTP9; IR20/RR16]	Failure to correctly update the online Register and hearing outcomes, makes the public register and associated products inaccurate resulting in less public protection
Partner contract changes [PTNR1; IR20/RR16]	(Historic partner contracts) A requirement to convert partner contracts to **worker** contracts will lead to significant costs for the HCPC due to changes in how employment law is interpreted.
Partner contract changes – future. [PTNR2; IR20/RR16]	Future Partner costs are increased due to enhanced rights, terms and conditions resulting from NMC case, impacting the HCPC budget.
IT skills, capacity and resources [IT5; IR20/RR16]	Failure to ensure that sufficient IT and digital skills, capacity, processes and resources with clarity on responsibilities, are in place to meet organisational expectations, manage InfoSec threats and deliver the corporate plan.

4. Directorate risk overview: Corporate Affairs

Chair and Chief Executive Office

4.1 A new Head of Governance is now in place and the balance of responsibilities between Governance and the Chair and Chief Executive Office is expected to remain as currently established, preventing any potential gaps or overlaps in processes and support. [GOV10; IR9/RR6].

Information Governance and Cyber Security

4.2 Following the successful migration from ISO27001:2013 to ISO27001:2022 during April–May 2024, the previous risk titled *"Failure to successfully migrate…"* [ICS7; IR9/RR6] has been updated to *"Failure to maintain ISO27001:2022 certification"* [ICS7; IR9/RR4]. The focus now shifts to ongoing compliance and maintaining certification under the new standard, where active searching for vulnerabilities is even more important.

4.3 As the organisation begins to selectively adopt AI products and services, a new risk has emerged around the potential accidental sharing of personally identifiable information (PII) or sensitive data with large language models (LLMs) or other services [ICS15; IR16/RR12]. While the HCPC has been very specific about the AI we chose to use internally, AI use will expand generally. One supplier has already experienced an incident involving unauthorised use of AI with HCPC information; however, it is not believed that any HCPC PII was exposed.

4.4 A new risk has also been added concerning the unintended or unauthorised recording or transcription of confidential meetings [ICS14; IR12/RR12]. In one instance, a partner working across multiple organisations unintentionally recorded HCPC business activity due to default settings in their primary IT system. Another case involved an individual recording a meeting to generate a transcript. While these incidents raise concerns, we must also remain mindful of accessibility requirements, including the use of assistive technologies to support participation.

Quality Assurance and Feedback and Complaints

4.5 The risk relating to concentration on high-risk areas (recently changed from concentrating on remedial work) [QA1; IR16/RR6] continues to focus on regulatory areas, and mitigations in FTP have resulted in increased compliance with PSA standards. However, there is still a risk that low level issues may be missed until they have more significant impacts. A slight increase in resources will mitigate this threat. [QA3; IR12/RR9] may be merged into this risk when the residual risk levels match.

4.6 Feedback and complaints receive a wide range of input from applicants, registrants, witnesses, and complainants. These submissions are often not concisely written, requiring careful interpretation. Trend analysis has proven effective in identifying areas of concern and driving remediation. Operating this function requires a comprehensive understanding of the organisation's operations and both feedback volumes and freedom of information (FOI)/subject access request (SAR) requests have risen significantly. To support growing demand, resourcing for this function is being increased one full time equivalent

(FTE) post with shared capacity allocated to Information Governance to assist with SARs and (FOI) responses.

4.7 There is a consolidated risk relating to the organisation's ability to effectively receive, interpret, and act upon feedback and complaints. Relevant information may be obscured within broader communications or not appropriately escalated, leading to delays in response and resolution [QA7; IR12/RR8]. Additionally, maintaining a continuous and proactive feedback mechanism is essential for identifying recurring or emerging issues in a timely manner [QA6; IR16/RR9].

4.8 Failure to act on feedback—particularly from service users and stakeholders—could result in missed intelligence regarding failing activities, whether internal or external [QA5; IR16/RR12]. This risk underscores the importance of ensuring that feedback is not only captured and acknowledged but also translated into meaningful action.

Governance

4.9 Governance-related risks have continued to reduce as key processes become more embedded across the organisation. The risk associated with unclear reporting guidelines [GOV1; IR12/RR3] has decreased significantly, with the annual report and broader reporting processes now well established. The National Audit Office (NAO) has conducted the annual audit independently, without Haysmacintyre, and no issues have been identified to date.

4.10 Governance controls relating to the ELT and the Council [GOV4; IR9/RR3] have also matured, with supporting processes now firmly in place and the successful replacement of four Council members during 2024-25. A KPI for Council paper submission deadlines is planned to further strengthen oversight.

4.11 The internal whistleblowing process [GOV6; IR12/RR6] is now well embedded, with annual training on anti-bribery and fraud actively monitored. This risk has reached its target rating, reflecting strong internal controls and organisational awareness.

Partners

4.12 The partner project continues to progress, although the scope of work has not significantly changed, future costs are expected to rise following the Harpur Trust Supreme Court decision [PTNR8; IR16/RR12]. Additionally, past partners have a limited window to claim payment for previous work [PTNR9; IR15/RR15], with the opportunity diminishing over time. The financial impact remains uncertain, with a wide range between full and minimal uptake.

4.13 Partner performance [PTNR5; IR12/RR8] is being restructured to reflect the distinct needs of the three core regulatory departments. Training and operational requirements vary across these streams, and separating performance oversight will support more targeted management and development.

Communication

4.14 Digital service availability [COM3; IR9/RR9] remains a concern due to the complexity of maintaining accessibility across a wide range of users, ongoing technical upgrades, and multiple language requirements. The appointment of a

new digital officer is expected to improve coordination of system changes and promote best practice across platforms.

4.15 There is also a reputational risk associated with the handling of sensitive topics [COM10; IR6/RR6]. Poorly crafted written or verbal communications, or statements open to misinterpretation, could negatively impact stakeholder perceptions of the HCPC. This risk applies even to trained staff, particularly in spoken communications, and highlights the need for careful messaging and ongoing awareness.

4.16 Our relationship with professional bodies remains strong [SR2; IR16/RR9], supported through consistent engagement, including quarterly meetings and the Professional Body Forum. This joint forum is attended by the majority of organisations and plays a key role in maintaining collaboration and alignment.

Professionalism and Upstream Regulation

4.17 There remains a risk that important external intelligence may not reach the appropriate individuals within the HCPC to prompt timely and effective action [PUSR2; IR12/RR12]. This reflects a lack of fully established processes for recording, sharing, and responding to such information. The post-mitigation risk rating has fluctuated, with likelihood increasing from 3 to 4 and returning to 3, resulting in a current rating of 12. The recent departure of the head of department contributes to ongoing uncertainty in this area.

4.18 Separately, the risk of limited understanding among professionals regarding new or updated standards has decreased [PUSR1; IR4/RR4], following a successful rollout last year. The effectiveness of the approach is supported by findings from a previous internal audit conducted by BDO.

5. Directorate Risk Overview: Education, Regulation and Regulatory Standards

Education

5.1 Education carries several inherent risks related to public protection, which sit at the lower end of the Medium/High range but are mitigated down to the lower end of Medium post-mitigation. One key risk is the reliance on staff with sufficient expertise to ensure the current model operates effectively [EDU23-6; IR12/RR6]. This is being addressed through succession planning, with an automated reporting solution also proposed to support consistency and reduce dependency on individual knowledge.

5.2 Availability of suitable partners for education processes [EDU-13; IR9/RR6] remains a challenge, particularly within smaller professions where conflicts of interest are harder to avoid. This risk is compounded by recent changes to partner contracts, which may discourage participation and make appropriate assessments more difficult.

5.3 There is also a minor concern that ongoing, incremental improvements to the operational model [EDU23-9; IR4/RR4] could gradually lead to divergence from its core principles. This risk has been acknowledged and accepted, with related considerations captured under [EDU23-8; IR8/RR6].

Registration and Continuing Professional Development (CPD)

5.4 The increasing volume of international applications has highlighted a growing risk of registrant fraud [REG2; IR16/RR12], particularly through potential plagiarism. Registration Assessors have identified recurring paragraphs across applications, suggesting copied content related to applicant experience. The implementation of Turnitin to detect plagiarism has resulted in more potential fraud being detected, resulting in increasing the inherent likelihood from 2 to 4. The inherent risk score has therefore increased from 8 to 16. Post-mitigation likelihood has also risen from 1 to 3, resulting in a residual risk of 12. Addressing suspected plagiarism has introduced additional operational processes and is a focus of the changes to the international assessment process that are in progress this year. We expect this risk post-mitigations risk score to reduce further once these changes come into effect and are embedded.

5.5 Current and future technology-related risks within Registration [REG3 and REG4; IR16/RR9] have been merged into a single risk concerning system or technology failure. This includes both current system functionality and the rollout of upgraded features. The risk level remains unchanged following the merge, reflecting consistent exposure across both areas. The registration area is dependent on fully functioning IT systems. No additional operational risk is recorded.

5.6 Reporting risks [REG13; IR20/RR9] have decreased due to a shift away from manually populated spreadsheets in favour of customer relationship management (CRM)-generated dashboards and PowerBI reports. Further dashboard development is planned to expand coverage across registration processes.

5.7 A capability risk related to partner recommendations [REG15; IR12/RR12] has increased, particularly in relation to evaluating positive recommendations. While initial assessments focused on negative decisions, incorrect positive recommendations pose a greater potential risk to public safety. The pre and post-mitigation risk remains at 12 until new checking mechanisms are introduced.

Insight and Analytics

5.8 Data quality remains a concern for both legacy data (pre-2025) and future data collection, particularly around definition and validation [I&A2 and I&A3; IR15/RR12]. These risks are being merged into a single item. To support improved reporting, minimum data sets are being developed across additional areas of the organisation, along with data stewardship and ownership across domains, maintaining accurate data dictionaries and documentation to enhance traceability, and data profiling to have insight into the health of our data.

Policy and Standards, EDI matters

5.9 The Policy and Standards operational risk register underwent a substantial review. A key change was made to the risk around legal advice documentation [P&S20; IR10/RR5], which now reflects the risk of failing to consult stakeholders during development and decision-making, rather than issues with documentation alone.

5.10 A reputational and operational risk remains around commissioned research [P&S22; IR9/RR3], where lack of strategic planning can result in missed opportunities and undermine the credibility and impact of research intended to support regulatory improvement and sector insight. Colleagues with experience of research commissioning are now in place and a new research governance process have been developed along with other mitigations.

5.11 A new risk was added concerning the HCPC's response to public inquiries and Reviews [P&S25; IR12/RR8], following concerns about the absence of a detailed response process. A public inquiry manual is being developed, and learning from other inquiries is acted upon to improve our response.

5.12 The Welsh language scheme risk [P&S24; IR12/RR12] has been revised to reflect a shift from project failure to long-term compliance. With the scheme largely implemented, the remaining technical requirement is now considered a web development issue and is likely to be transferred to Communications or Business Change.

Regulatory Development and Performance

5.13 Two risks have been identified in this new department, where remit boundaries are loosely defined and overlap with Business Change, Projects, and IT. Mitigations include ensuring clarity of role and this is enabling the rapid trialling and development of solutions to business challenges [RDP2; IR12/RR8], as well as swift rollout of those solutions across departments to support fully functioning processes [RDP3; IR12/RR4].

6. Directorate Risk Overview: Fitness to Practise and Tribunal Service

6.1 Efforts to improve the efficiency of FTP processes are captured under [FTP1; IR9/RR9] and [FTP2; IR16/RR12], which may be merged once residual risks align more closely. Case volumes risk [FTP3; IR16/RR9] reflects the challenge of managing high volumes, with reduced impact but increased likelihood due to rising caseloads. These risks have been mitigated by delivery of the FTP improvement project; new operating model in place for FTP; introduction of frontloaded and streamed investigations are in place or were being fully rolled out over the year.

6.2 While gradual growth in case numbers is expected as registrant numbers increase [FTP5; IR12/RR12], small, sudden surges potentially could occur and may require tailored responses. Outsourcing cases helps manage internal workload but introduces the requirement related to managing external quality assurance and safeguarding public protection, [FTP13; IR20/RR15].

7. Directorate Risk Overview: Resources

Estates (Office Services) and Facilities

7.1 As cloud migration progresses, reliance on full-service availability within office buildings has decreased. The risk previously focused on server room power failure has been broadened to cover the entire building [OFS3; IR8/RR4], with hybrid working enabling most staff to operate remotely, except for Estates, and some Registration and FTP administration teams.

7.2 The end-of-life replacement of building plant [OFS2; IR12/RR6] is being managed through a phased approach, starting with equipment at the rear of the building. This will involve some internal relocations.

7.3 AI usage presents a sustainability risk [OFS9; IR12/RR9], as large language models require significant processing power and storage, increasing energy consumption—even if not actively deployed. Free trials offered by vendors suggest capacity is available, but environmental impact remains a concern.

7.4 Lone worker safety [OFS10; IR8/RR6] has been identified as a risk, particularly for FTP hearings officers, panel members, and staff in professionalism and upstream roles who regularly work off-site. Regular communication with managers, known locations and additional controls on transport selection are in place.

Finance and Procurement

7.5 The Payroll team has received additional resource [FIN7; IR12/RR6] in preparation for managing partner payments, strengthening resilience across both employee and partner processes. This has reduced the post-mitigation risk from 8 to 6.

7.6 Vendor management [FIN5; IR9/RR6] remains a focus, with continuous contract monitoring essential to ensure service delivery. The introduction of the Procurement Act 2023 and a new contract management module in Business Central will support improved oversight and compliance.

7.7 The shift from six-monthly to quarterly direct debit payments [FIN11; IR15/RR4] may temporarily misalign internal and external processes, requiring dual regimes until all professions complete the renewal cycle. While this increases the frequency of payment failure opportunities, the lower quarterly amounts may reduce the risk of registrants exceeding overdraft limits.

7.8 Reporting on deferred income still requires manual intervention until full Business Central functionality is rolled out.

Information Technology

7.9 The risk of a successful cyber-attack remains a constant concern [IT7; IR20/RR12], particularly in light of recent SMS toll fraud activity. More resourced organisations have experienced significant breaches, underscoring the importance of continued vigilance against both accidental and deliberate threats

7.10 A new risk has emerged [IT9; IR12/RR12] following instances where IT suppliers have taken unilateral action—such as withdrawing services from specific regions—without notice. This has led to fallback paper-based processes, which, while low impact for most users, can be challenging for those affected.

7.11 User permissions [IT2; IR12/RR8] present an ongoing risk due to the complexity of managing access across hundreds of roles. Mitigation involves collaboration with HR and Information Governance, supported by new audit processes currently being rolled out.

7.12 The IT team has undergone restructuring [IT5; IR20/RR16], with several new staff in place. However, recruitment for the automation role has only recently

been successful, reflecting the high competition for candidates with this technical capability.

Human Resources, Learning and Development

7.13 Recruitment remains a challenge [HRD1; IR12/RR9], though the expansion of the HR team has slightly reduced the post-mitigation risk from 12 to 9. Hybrid working continues [HRD3; IR8/RR4], with HCPC currently meeting its internal 20% office attendance requirement. Recent legislative changes may affect this, (up to two requests per year for changes in working pattern from the first day of employment) but the organisation's flexible approach supports retention. A related strategic risk is held by the Senior Leadership Team [SLT20; IR9/RR6].

7.14 Staff morale [HRD4; IR12/RR8] is generally strong and at target level, supported by quarterly Pulse surveys. As of June 2025, the HCPC reported an 80% retention rate.

Projects and Business Change

7.15 Balancing large corporate projects with smaller departmental initiatives [PBC12; IR8/RR4] presents a challenge, as lower-priority projects may be delayed due to resource constraints. Increased project management capacity is being introduced to improve delivery across all areas.

7.16 Change management [PBC9; IR12/RR3] may be affected if business requirements and their cross-organisational impacts are not well understood or maintained—an issue closely linked to the product management knowledge risk.

8. Senior Leadership Team

8.1 A key strategic risk carried by the Senior Leadership Team is the joint responsibility for patient safety [SLT9; IR16/RR9], which depends on the effective delivery of core regulatory functions and business-as-usual activity. Fitness to Practise remains a resource-intensive area [SLT15; IR12/RR8] and the need to invest in this area to maintain performance to manage increases in the number of complaints may reduce funding available for other areas.

8.2 The loss of corporate memory [SLT18; IR9/RR6] is an ongoing concern, as staff turnover can lead to gaps in understanding past decisions and processes. The Senior Leadership Team is actively addressing this through improved retention strategies, process mapping and the development of centralised stores of organisational knowledge.