Audit and Risk Assurance Committee

Meeting Date	16 September 2026
Title	Unified assurance report September 2026
Author(s)	Anna Raftery, Head of Assurance and Compliance
Executive Sponsor	Claire Amor, Executive Director of Corporate Affairs

Executive Summary

This report summarises assurance activity in the reporting period across the HCPC. It seeks to act as a source of assurance and intelligence to the Committee. The report is based on the three lines of assurance model. While it seeks to be comprehensive, the report may be limited by the quality of information provided to the Assurance team.

Due to the risk management audit recommendations and resource availability the risk and assurance meetings did not take place for Q1 2026-27. Instead, a full review of 140+ operational risks was undertaken, and a new assurance mapping tool was developed.

This paper forms part of the assurance framework, delivering the requirement to report on the assurance map and assurance workplan.

Overall, the assurance rating for this period is **medium**.

This paper covers the period of April 2026 to July 2027

Appendix 1: 2026-27 Workplans (standing attachment)
Appendix 2: Risk Appetite Statement (standing attachment)
Appendix 3: Assurance Map Pillars
Appendix 4: NAO Cyber Questions mapping

Action required	The Committee is asked to review the information provided and seek clarification on any areas.
Previous consideration	This is a standing item considered at each meeting of the Committee. This paper was reviewed by ELT.
Next steps	The next unified assurance report will go to the Audit and Risk Assurance Committee (ARAC) in November 2026.

Financial and resource implications	None as a result of this paper.
Associated strategic priority/priorities	Supporting healthcare workforce development through proportionate, agile regulation Technology-enabled regulatory excellence and organisational sustainability
Associated strategic risk(s)	All
Risk appetite	Regulation - measured Compliance - measured People - open
Communication and engagement	None as a result of this paper.
Equality, diversity and inclusion (EDI) impact and Welsh language standards	This paper includes the assurance of HCPC EDI as related to regulatory and business practices.
Other impact assessments	This paper includes the assurance of HCPC data and sustainability as related to regulatory and business practices.
Reason for consideration in the private session of the meeting (if applicable)	Not applicable

Unified Assurance Report September 2026

Contents

1 Executive Summary

1.1. The September 2026 unified assurance report provides an overview of the HCPC's assurance position across all three lines of defence, reflecting activity and findings from Q1 of 2026–27, along with a year-to-date overview. Overall, the organisation's assurance level remains **Medium**, indicating that core controls are in place and generally effective, but further strengthening is required in targeted areas.

> **Medium**: Concerns over the adequacy or compliance of the controls in place in proportion to the risks, improvements required.

1.2. Due to the risk management audit recommendations and resource constraints the risk and assurance meetings did not go ahead in Q1 2027-26.

1.3. First line checks continued in the three regulatory areas, providing insight on performance and areas for improvement.

1.4. The quality assurance (QA) workplan was amended following Executive Leadership team (ELT) feedback to prioritise activities in the Fitness to Practise (FTP) department, including developing new customer service first line checks, and a lessons learned review on the mobilisation of FTP Legal Services.

1.5. The new Information Governance and Risk Lead started in July 2026 and will be taking over the management of Information Governance, ISO 27001 compliance, and operational risk management. Recruitment for a new Risk Officer role to support this work is ongoing.

2 Risk and Assurance Overview

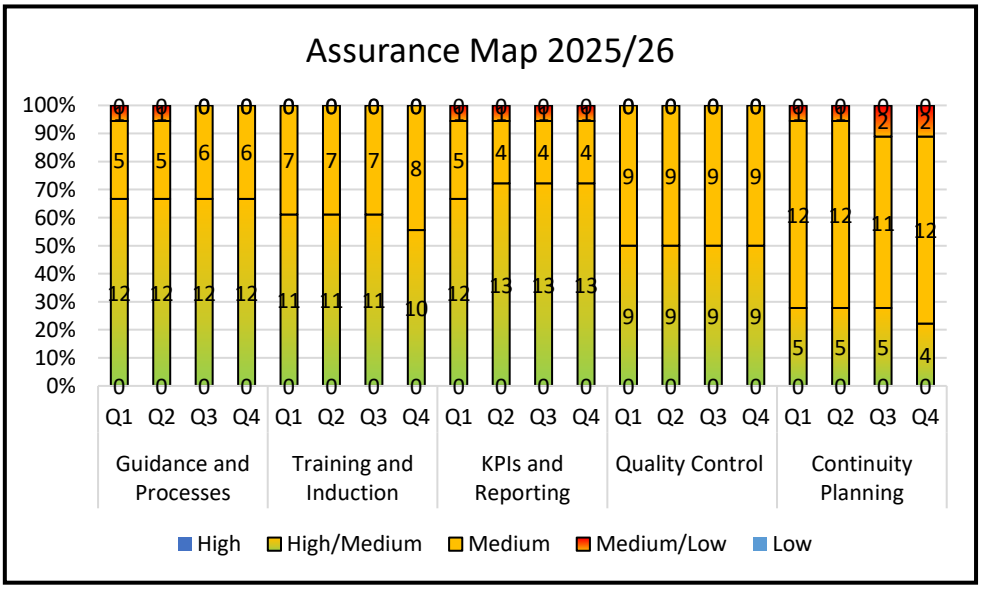
2.1. Due to the operational risk register audit and subsequent recommendations, combined with the departure of two thirds of the risk management resource the Q1 2026-27 risk and assurance meetings did not go ahead.

2.2. Instead, a new self-assessment assurance mapping tool was developed and is now being tested with the department heads. This tool asks that each of the five pillars are scored by the function owner, followed by a space for commentary to support the assessment. They are then asked to decide what the overall assurance level is.

2.3. The aim for this tool is that we will continue to complete a full assurance mapping exercise annually for each department, and in between the self-assessment tool will be completed. This tool will be managed by the Risk Officer when in place, including ensuring evidence is verified.

2.4. For the operational risk register (ORR) we prioritized a full review of all operational risks with a view to either close/accept, moved to department risk registers, or keep. Through this exercise we identified many duplicate, superseded, or low level risks which left us with 25-30 for review. These risks will be owned by SLT members and overseen by the group. Further details of the ORR improvement can be found in the operational risk register update August 2026.

2.5. For reference, here are the assurance ratings to date:



2.6. Due to this prioritisation the assurance level has not changed this quarter. Our overall assurance level is Medium, which means we have good controls in place, but there is still work to do to make them stronger. This rating is not about performance; it shows how secure and reliable our processes are.

Medium: Concerns over the adequacy or compliance of the controls in place in proportion to the risks, improvements required.

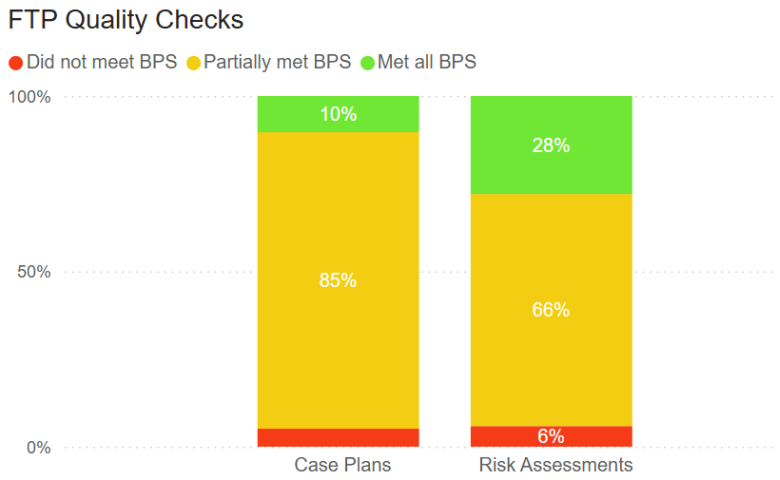
Regulatory First Line Assurance

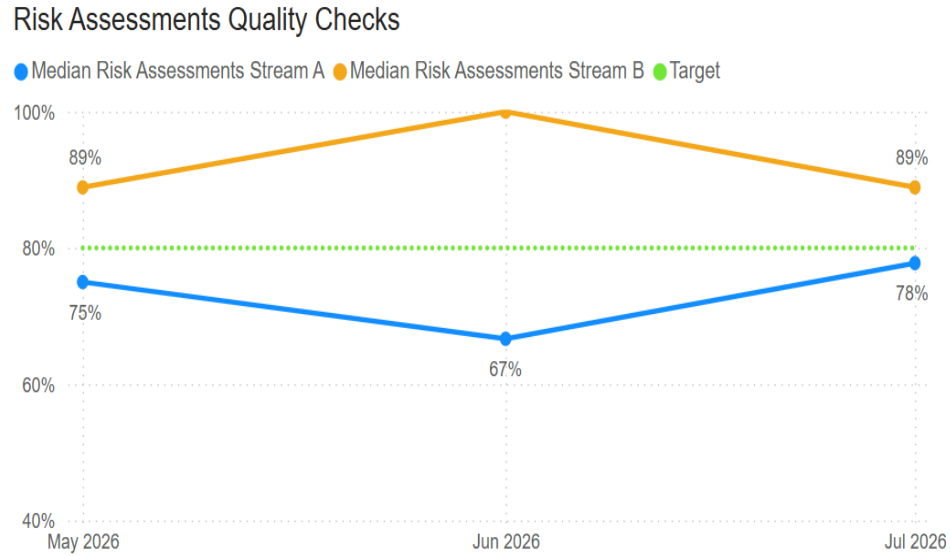
3 FTP and Tribunal Services (TS): Case Progression and Quality

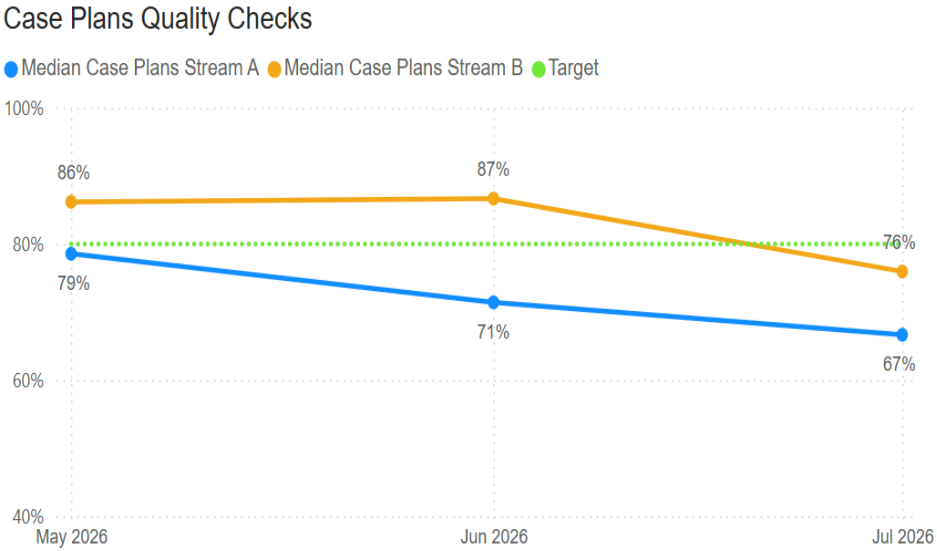
3.1. Between May and July 2026, 136 quality checks were completed on both risk assessments and case plans against the best practice standards (BPS)[1].

3.2. Risk Assessments

- The median risk assessment score across both Stream A and Stream B was at least 67% for each month during this period.







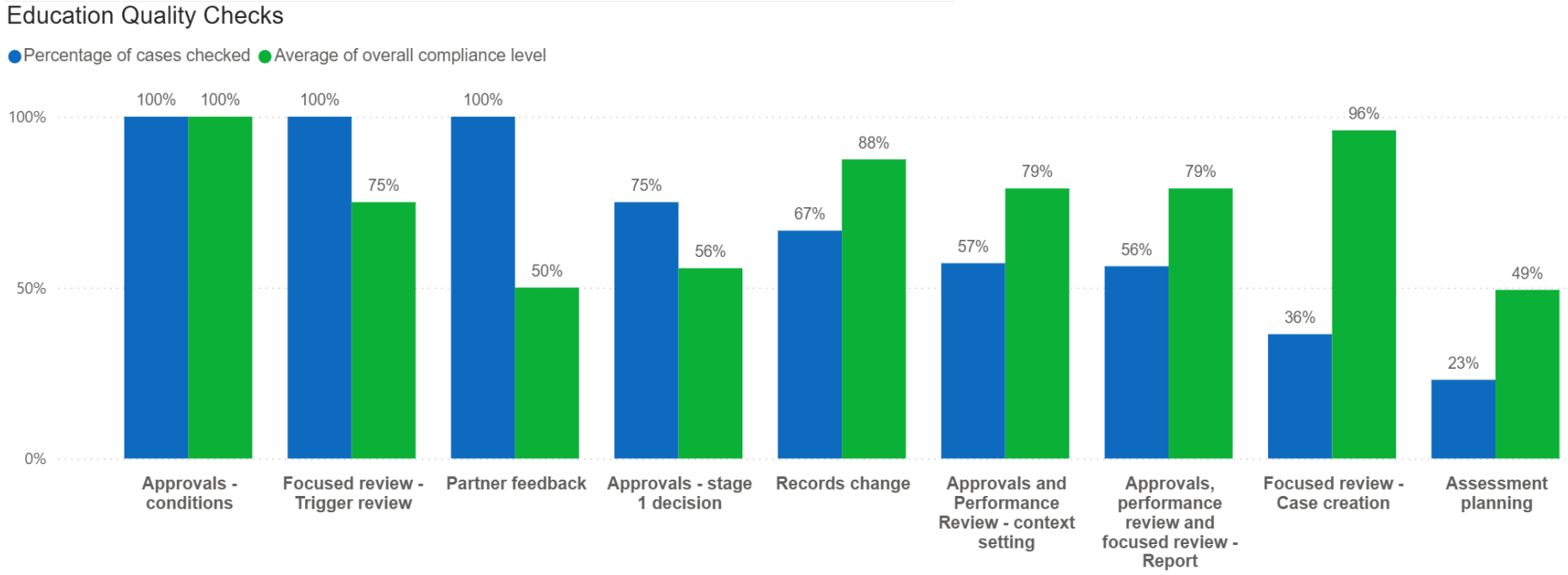
[1]Median scores show the quality checks (QC) score % of meeting BPS.

4 Education, Registration and Regulatory Standards (ERRS): Education

4.1. Between May and July 2026, 83 cases were quality checked by the Education department. These checks took place at nine different steps of the Education process.

4.2. The average overall compliance level was 72% across the nine process steps. Timeliness was the biggest factor for compliance levels being less than 100%. The Head of Education also noted that assessment planning and professional body engagement are areas needing improvement.

4.3. None of these findings impacted on the quality of the recommendation or the overall decision.



5 ERRS: Registration

5.1. In Q1, the Registration Quality Assurance team (RQAT) completed two audit exercises. Assurance of the contact centre process and readmissions process.

Contact Centre

5.2. The audit of the contact centre service followed the implementation of the Five9 telephone system in November 2025, which enables call recording and quality review. The audit aimed to assess call quality and evaluate how effectively customer queries and requests were resolved.

5.3. **Sample and Assurance:**

A sample of **355** calls (95% confidence level, 5% margin of error) was randomly selected. Of these, 328 were handled by Registration Advisors (RAs) in the Contact Centre team and 27 by RAs from other teams.

Call Category	Volume
Registration Renewal	126
Registration International	96
Registration UK	78
Registration Check	41
Registration CPD	14
Total:	**355**

The analysis was conducted at a 95% confidence level to ensure reliability and representativeness of findings.

Key Findings
Security checks effectively identified the caller. However, guidance on this area is not clear or comprehensive, and as a result, security processes vary between caller handlers.
Calls were inadequately documented. Inadequate evidence and audit trail risks the timely and effective progression of calls and /or applications.
Responses to queries were accurate and resolved the request. Callers were not always directed to the website to obtain full details on complex topics.
Communication was clear and professional.
The majority of calls were answered with the expected opening content.

Readmissions

6.4 The readmission audit aimed to assess the quality and consistency of the readmission application process

6.5 **Sample and Assurance:**

A sample of **268 applications** (95% confidence level, 5% margin of error) was randomly selected. Of these, 66 were long readmissions, and 202 were short readmissions.

Category	Volumes	Volume %
Long Readmissions	66	25%
Short Readmissions	202	75%
TOTAL	**268**	**100%**

Key Findings
Evidence that embedded first-line checks are having the desired impact. Multiple errors had already been identified and corrected before auditing.
Areas with a higher likelihood of errors (minor data entry mistakes, incorrect or missing statuses and fields) tend to have lower levels of risk.
A small number of errors had the potential to pose significant regulatory risk, such as potential protection of title (POT) concerns, inadequate verification of return to practice (RTP) and incorrect payment amounts.
Customer service errors and delays were linked to attention to detail – failing to identify data in forms obscured by Adobe layering, and not checking for missing or unacceptable documentation carefully.

The assurance rating for both audits was:

High/Medium	Generally, a good process is in place. However, some minor weaknesses have been identified in the process or areas of non-compliance which may put achievement of regulatory or business objectives at risk.

Note: a first-time audit cannot provide full assurance as evidence of consistency over time is needed

6 Quality Assurance

Quality Assurance (QA) Activity: May – August 2026

Education Programme Records
Commenced March 2026, Completed May 2026

The HCPC has a legal responsibility under the Health Professions Order 2001 to "maintain and publish a list of courses of education or training, qualifications and institutions". The Education department ensures that the HCPC continues to meet this statutory requirement by maintaining an accurate record of education programmes.

This review shows strong evidence of improvements being made to the processes since the previous QA review in 2025 particularly in establishing robust process controls and strong managerial oversight of cases, resulting in high levels of compliance with the process guidance for both approval and record change processes, and high levels of accuracy for the list of approved programmes.

The review identified multiple opportunities to improve audit trail and decision-recording practices across various levels of the team, including management. This has had an impact on the decision-making process regarding the broader quality impact of the programme record changes. The review also identified two programme records, where the first intake dates appeared incorrectly on the list of approved programmes.

For these reasons, this review has been given a **Medium** assurance rating. Seven recommendations have been made and accepted by the Education department.

HCPTS - Review Hearing Scheduling
Commenced late April 2026

The purpose of this review is assess the process for scheduling review hearings. This review will also focus on understanding what areas of the process could impact upon timely scheduling.

This review is due to report to ELT in September 2026.

FTP Registrant Assessor Process
Commenced May 2026, Reported to ELT in August 2026

Registrant assessors can be appointed to give advice on matters of professional practice arising in connection with any matter that a Practice Committee is considering. Registrant Assessors are in existing HCPC Partner roles (e.g. Registration or CPD assessor roles) and give opinion evidence on matters within their area of expertise in the form of a report – they generally do not give oral evidence, are not cross-examined and do not testify.

The process for obtaining Registrant Assessor reports is lengthy and the review found it takes approximately four months on average to obtain a report. The internal guidance for this process was last updated in 2017 and does not reflect the current process. This has resulted in an inconsistent approach to obtaining registrant assessor reports, which was one of the main concerns highlighted in the review. Inconsistencies in how registrant assessors are instructed can lead to lower quality reports, which increases the risk of adjournments.

The review of registrant assessor reports found that for each criterion, more cases met the criterion than did not. However, the review also found that relevant documentation was not always saved to the Nexus record and opportunities for giving

feedback to registrant assessors or requesting amendments were not always taken.

The assurance rating for this review is **Medium/Low**. Seven recommendations have been made and accepted by FTP.

HCPTS Quality Checks Workshop
June 2026

In June 2026, the Quality Assurance (QA) Team facilitated a workshop with operational managers and managers from HCPTS. The aim was to better understand the risks associated with hearings and scheduling processes and help develop appropriate first line checks to mitigate risks and assure the process.

In the workshop, progress was made in identifying the risks in the current process and defining QC criteria to address these risks. Four recommendations have been made by the QA team to ensure the process is robust, proportionate and effective, and HCPTS aim to commence the new process in October 2026.

FTP Legal Services Project – Lessons Learnt Review
Commenced June 2026

In April 2026, the People and Resources Committee (PRC) requested that the QA team undertake a lessons learnt review of the Legal Services project. A review of documentation, workshop and interviews have been undertaken and will be reported to ELT in August 2026 and PRC in September 2026.

FTP Customer Service First Line Checks
Commenced May 2026

The QA Programme Lead has worked closely with FTP operational managers and Investigation team managers to develop a new set of first line checks to monitor and report on customer service. These first line checks will assess the quality of interactions with stakeholders alongside response times.

Following workshops and a pilot, the new set of first line checks was rolled out at the start of August with reporting to the Council to begin in September 2026.

FTP Racial and Religious Discrimination Review Commenced July 2026

In June 2025 the Department of Health and Social Care published the 'Lord Mann review of antisemitism and other forms of racism in the NHS and healthcare regulatory system'.

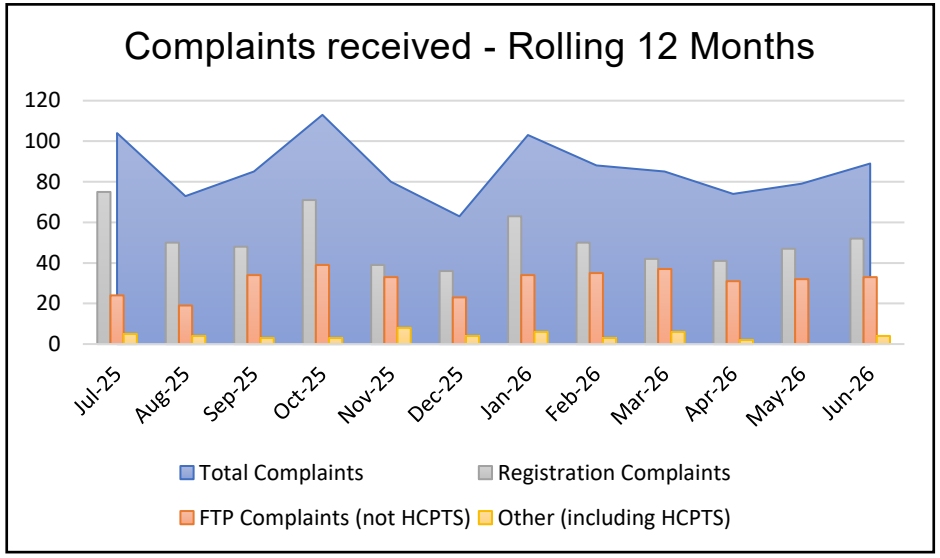
This review was commissioned by the Secretary of State of Health and Social Care and the Prime Minister in October 2025 and was focused on how the NHS and its regulatory system recognises, reports and tackles antisemitism and other forms of racism.

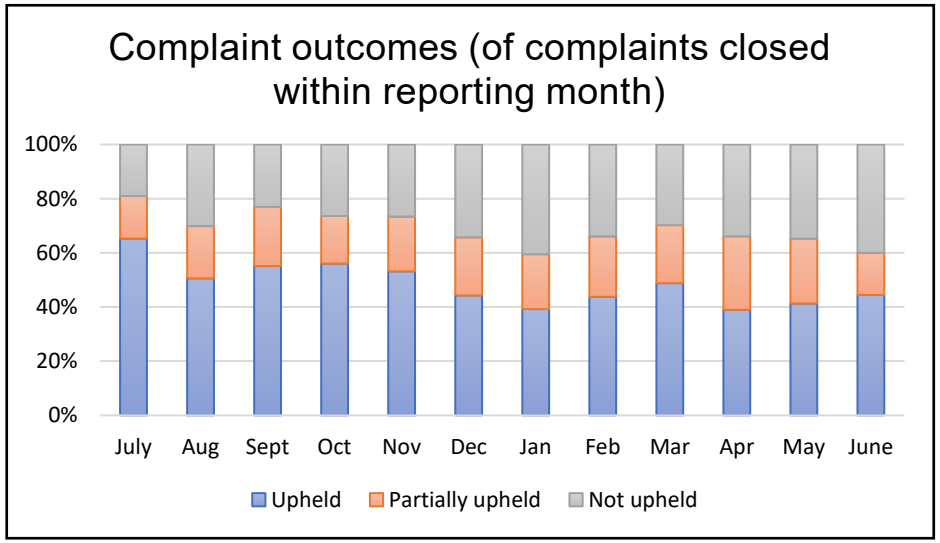
The ELT has asked the QA team to undertake a review of how FTP handle cases involving racial and religious discrimination. This review is intended to be an overview rather than an in-depth audit.

This is due to be reported to ELT in November 2026.

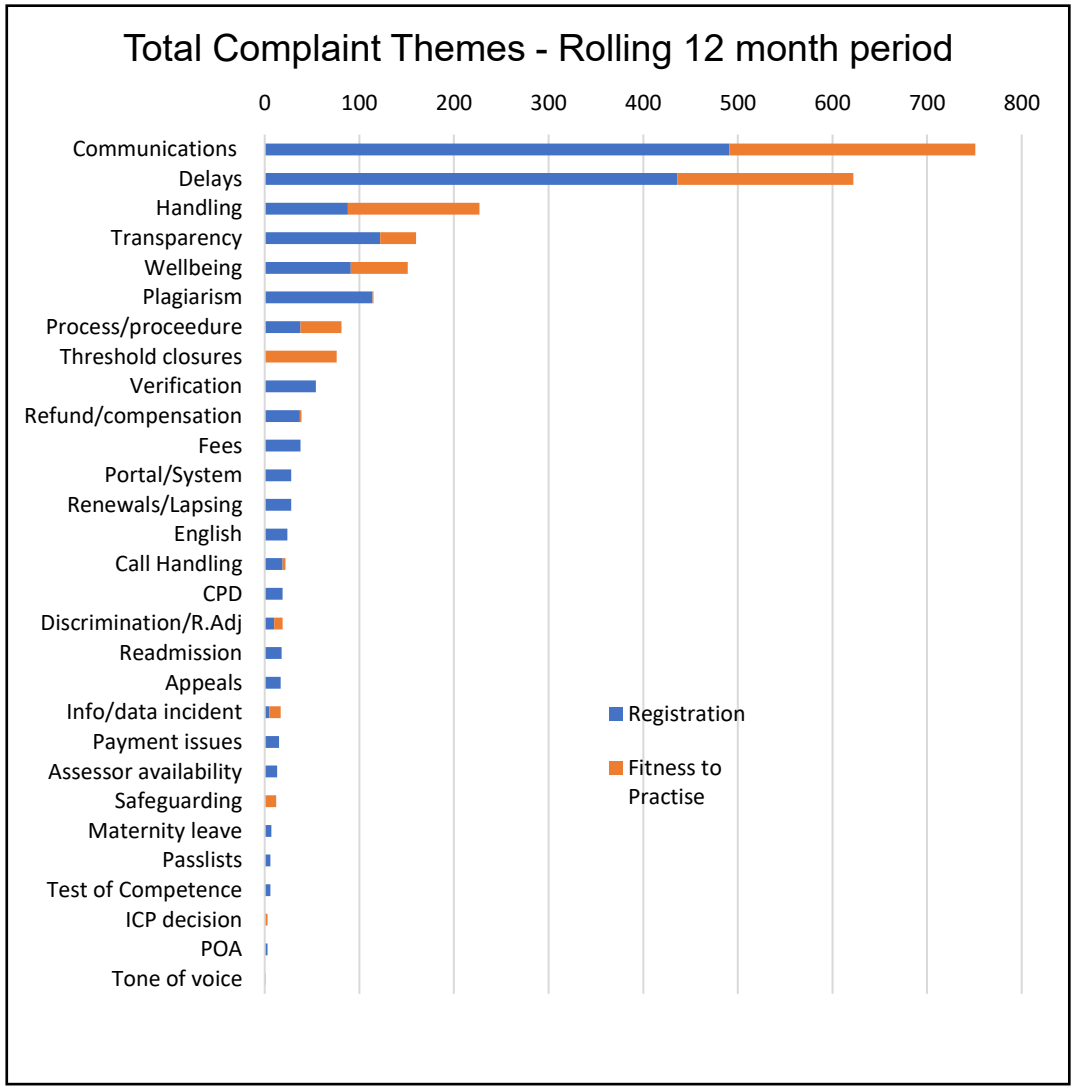
7 Feedback and Complaints

7.1. Complaints received between July 2025 and June 2026:





7.2. Complaint themes from July 2025 to June 2026:



7.3. The most common themes remained communications and delays with applications and case progression.

8 Risk and Compliance

Risk and Compliance 2026-27 workplan progress

8.1. The following non regulatory activity has taken place since the last ARAC report:

- Following the departure of the Chief Information Security and Risk Officer (CISRO) and the induction of the Information Governance (IG) & Risk Lead, the focus since the last report has been on handover, knowledge transfer, and onboarding activities to support a smooth transition.

- Information security induction training materials have been updated to incorporate enhanced data protection content, in response to feedback and recommendations from FTP.

- Mandatory information security training has been reviewed and divided into two separate modules: information security and data protection. The data protection module includes expanded content to strengthen staff data protection knowledge and awareness.

- Bi-weekly Network Transformation Project Board meetings continue to be held with IT and change management colleagues to oversee delivery, track progress, and manage associated risks and dependencies.

Serious Event Reports (SERs)

8.2. The are no current open SERs.

Whistleblowing, Fraud and Bribery monitoring

8.3. The Anti-Fraud and Anti-Bribery and Corruption mandatory trainings have been merged and refreshed for a more streamlined learning for staff.

Risk and Compliance Audits commentary

8.4. The next set of Risk and Compliance audits are ongoing. The DBS Renewal process is being evaluated. Addressing the more detailed requirements of the new ISO standard is potentially challenging.

Business Continuity and Disaster Recovery exercises and planning

8.5. With the Departure of the CISRO, the IG and Risk Lead has taken over management of ShadowPlanner v6 as our business continuity tool. Support is being provided by a QA Officer while the new Risk Officer recruitment is underway.

8.6. As part of the preparedness for ISO 27001:2022 audit, we are considering our business continuity, and disaster recovery, needs to ensure that our current tools remain suitable.

8.7. A test with Estates and Facilities is being planned for the next month.

Single Source Suppliers

8.8. The following contracts have been signed without competitive tender. These suppliers have been used before by HCPC or are offering specific services that are compatible with other functionalities that requires specific integration.

SSR No	**HCPC/SSR /2026/65**	**HCPC/SSR/2 026/66**	**HCPC/SSR/20 26/67**	**HCPC/SSR/ 2026/72**
Date	12/05/202 6	14/05/2026	11/06/2026	19/08/2026
Department	Facilities Manageme nt	IT & Digital Transformati on	Human Resources	Communicati ons
Tender Owner	Stefan Marin	Geoff Kirk	Fatima Ali	Adam Haxell
Description	Visitor Manageme nt System	Barracuda (Bytes) Web Application Firewall Extension	WDI Consulting	The Patients Association
Value	£17,500	£16,726	£29,999	£26,712
Duration	12 months	12 months	12 months	12 months

Third Line Assurance

9 PSA Performance Review 2026-27

9.1. The Professional Standards Authority (PSA) has now published the revised standards of good regulation in April 2026 with the new standards going into effect in July 2026. The General Chiropractic Council will be the first regulator assessed against the revised standards.

9.2. HCPC's 2026-27 performance review commenced on 1 April 2026 and will end on 31 March 2027. This is intended to be a monitoring year, and the PSA have advised that they intend to assess the HCPC in 2026-27 against the current standards. The HCPC will be assessed against the new standards from April 2027.

9.3. In July 2026, the Executive Director for ERRS, Head of Assurance and Compliance, and QA Programme Lead facilitated a workshop with members of the Senior Leadership Group to identify good practice to share with the PSA and to consider ways performance could be improved against the standards in 2026-27.

9.4. In October 2026, another workshop will be held to consider the new Standards of Ggood Regulation, identify new requirements, and begin planning for the 2027-28 performance review cycle.

10 Information and Security and ISO27001:2022; Anti-Fraud and Bribery

10.1. At the end of July 2026 the CISRO retired after 24 years at the HCPC. His legacy is the foundation for much of our assurance framework and will continue to support the improvements and changes to come.

10.2. The new IG and Risk Lead joined us in early July 2026 and received 3 weeks handover with the CISRO before his departure.

10.3. ISO 27001 recertification readiness review is underway to assess compliance, identify potential non-conformities, and highlight opportunities for improvement ahead of the recertification audit in March 2027.

10.4. A review of key governance policies and procedures is also in progress to ensure continued alignment with regulatory requirements and organisational objectives. This includes information governance, data protection, information security, business continuity, anti-bribery and corruption, and anti-fraud.

10.5. Recruitment is in progress for a risk officer. The role will in addition to its core responsibility also provide support for the ongoing management and maintenance of the ISO 27001 certification.

11 Information Governance

11.1. Summary of recent requests:

Requests	May-26	Jun-26	Jul-26
FOI	16	20	25
SAR*	12	11	17
EIR	0	0	0
Disclosure requests	15	13	12
Internal reviews	5	6	8
ICO complaints	1	0	1
Total Received	**49**	**50**	**63**
Total Closed	55	54	43
Responses within statutory timescale	53	50	41
Responses in breach of statutory timescale	2	4	2
% age within statutory timescale	96%	93%	95%

11.2. We received 19 data incident reports in the reporting period.

* Includes all data subject information rights requests

Appendices

Appendix 1 Workplans 2026-27
Quality Assurance

In 2026-27 we will…			Strategic aim (subject to change)	Cross organisational impact/input required	Start	Delivery
QA in FTP •Registrant Assessor Process •ICP adjournments •Streaming •Review Hearings Scheduling •AI usage - Redaction Tool *Advisory:* •Frontloading – First line checks	QA in Registration •Plagiarism Identification Process (co-working with Registration QA Team) •AI usage - EmailTree •Appeals •Support for Registration QA team's review of Non-Clinical Tests of Competence	QA in Education •Lessons Learnt Review (EHU – continuation from 25-26) •Performance Review •Stakeholder Intelligence *Advisory:* •Implementation of SETs– measuring success	Supporting Healthcare Workforce Development Through Proportionate, Agile Regulation	Education, FTP, Registration	Q1	Q4

Information Governance - ongoing improvements, business as usual (BAU) delivery an archive project Manage delivery of Archive project	Patients at the Centre of Smarter, Preventative Regulation	FTP, Registration, Policy, IT, I&A, Communications	Q1	Q4
Feedback and Complaints - ongoing improvements and BAU delivery	Patients at the Centre of Smarter, Preventative Regulation	FTP, Registration, Communications, Governance, Policy	Q1	Q4
Input into 'single CRM', 'website and portals', and 'customer contact phase 2' projects to improve ways of working in Feedback and Complaints and Information Governance Provide assurance expertise as required for ongoing change projects	Technology-Enabled Regulatory Excellence and Organisational Sustainability	Business Change IT, FTP, Registration, Communications	Q1	TBC
Risk - Manage the Strategic and Operational Risk Registers (BAU and improvements) Embed new strategic risks and approach Delivery Risk Appetite review and embed outcome	Supporting Healthcare Workforce Development Through Proportionate, Agile Regulation	All	Q1	Q4
PSA - Performance Review 2024-25 (monitoring year) Manage the relationship with the PSA for the 2024-25 Monitoring Performance Review	Supporting Healthcare Workforce Development Through	All	Q1	Q4

Embed new PSA standards	Proportionate, Agile Regulation			
IA - Induct and business partner with new Internal Audit team (RSM) Manage delivery of full IA workplan	Supporting Healthcare Workforce Development Through Proportionate, Agile Regulation	All	Q1	Q4
ISO27001:2022 and Information security - Manage ISO 27001:2022 delivery and audit Deliver monthly audits on Sentinel and NCSC tools online with IT security engineer	Technology-Enabled Regulatory Excellence and Organisational Sustainability	IT All other departments	Q1	Q4
Business continuity - Deliver departmental Business Continuity tests Manage ShadowPlanner, including a content review, improved comms, and effective guidance	Technology-Enabled Regulatory Excellence and Organisational Sustainability	All	Q1	Q4

RSM Internal Audit Plan 2026-27

Area	Audit approach	Proposed timing	Proposed Audit and Risk Assurance Committee Reporting
Finance			
Key Financial Controls – Accounts Receivables / Registration Fees Data analytics will be utilised to test compliance against processes outlined in policies and procedures. As part of the review, we will consider the following areas: • The controls in place to ensure registration fees are received promptly and timely and are accurately recorded in the database and systems. • The methods used to make payments and how HCPC monitors and tracks the methods used. • The processes for following up on payments once they are past the due date. • How registrants are removed/paused from the register for late payment of registration fees and the processes for getting registrants back on to the register following payment. • Debtor management processes in place including month end procedures. • Registration fee income reconciliations are completed promptly and in line with segregation of duties. • Monitoring and reporting arrangements to relevant oversight Groups and / or Committees. **Strategic Risk – 5.a – The resources we require to achieve our strategy are not in place or are not sustainable.**	Risk based	November 2026	March 2027

Area	Audit approach	Proposed timing	Proposed Audit and Risk Assurance Committee Reporting
Business Risk – The Council does not achieve a sustainable budget or the planned financial benefits.			
Quality and Performance			
Data Quality and Management A new corporate strategy has been developed at the HCPC and is due to be embedded from 2026. The review will assess whether performance measures are clearly defined and communicated, whether data collection and reporting processes are robust and reliable, and whether underperforming indicators have appropriate actions in place. We will also evaluate the adequacy of reporting arrangements and how effectively performance is monitored across operational groups, committees, and the organisation. Key performance indicators will be agreed with management. **Strategic Risk 1 – 3.a – Quality of our data leads to assumptions or gaps in understanding, and therefore inadequate or uninformed decision making.** **Strategic Risk - 3.b – We are unable to maximise our use of the data we hold to share insights to protect, promote and maintain the health, safety and well-being of the public.** **Business Risk – If data is inaccurate, incomplete or outdated, leaders may make strategic or operational decisions based on misleading information.**	Risk based	June 2026	September 2026
Information Technology			
Incident Management and Business Continuity An audit on Incident Management and Business Continuity will assess the robustness of plans in place, ensuring they cover critical functions, the testing of these plans, key roles and responsibilities and the assurance mechanisms in place, that in the event an incident arises, the organisation are ready to deploy the plans. This review will be supported by specialists from our Technology Risk Assurance team. This will build on any related elements from your work in 2025/26 on Cyber Security. **Strategic Risk 5.a - The resources we require to achieve our strategy are not in place or are not sustainable.**	Risk based	April 2026	June 2026

Area	Audit approach	Proposed timing	Proposed Audit and Risk Assurance Committee Reporting
Business Risk – There may be extensive disruption to both service delivery and the invigilation of the online registration assessment, resulting in significant delays, cancellations, and concerns around the integrity of the process.			
Contingency Audit			
We have included a contingency audit allocation as part of the internal audit plan. This provision allows the Internal Audit team to be agile and responsive to emerging risks, regulator changes, or changes to organisational priorities that may arise. Areas for consideration include: • Corporate Complaints – Strategic Risk 4 • Procurement – Strategic Risk 5.a. • AI Implementation – Strategic Risk 3.a. and 3.b • Registrants Wellbeing – Strategic Risk 6 • Regulatory Audit – Registration – Strategic Risk 1	Risk based	September 2026	November 2026
Other Internal Audit Activity			
Follow Up: To meet internal auditing standards, and to provide assurance on action taken to address recommendations previously agreed by management.		At each Audit and Risk Assurance Committee	
Management: This includes annual planning; preparation for and attendance at Audit and Risk Assurance Committee; regular liaison and progress updates; liaison with external audit and other assurance providers; and preparation of the annual opinion.		Throughout the year	

A detailed planning process will be completed for each review, and the final scope will be documented in an Assignment Planning Sheet. This will be issued to the key stakeholders for each review.

Appendix 2 Risk Appetite Statement

HCPC Risk Appetite Statement November 2023

Regulation – Measured (Registration, Education, FTP, Policy & Standards)

Our focus is on long term and lasting quality in our regulatory delivery. We prefer safer delivery options for meeting our requirements as a regulator, accepting a measured degree of residual risk and choosing the option most likely to result in successful delivery in order to continue as an effective regulator.

It is **essential** that mitigations to ensure ongoing public protection are in place as a foundation of taking risks to delivering regulatory requirements.

Influence/Leadership – Seeks (Engagement, comms, profile, reputation, influence)

We are willing to take decisions which are likely to bring additional scrutiny of the organisation. We outwardly promote new ideas and innovations where potential benefits outweigh the risks.

It is **essential** that the HCPC's voice is not perceived to be party political. The HCPC is neutral as a public body.

Compliance – Measured (PSA, ISO, ICO, Environmental, H&S, etc)

We have a preference for safe delivery options with little residual risk. We want to be reasonably sure we would win any challenge. Data protection, IT and cyber security are covered by this risk type.

It is **essential** that the long-term achievement of PSA standards is assured.

Financial – Measured (Finance, VFM, Estates)

We will pursue safe delivery options, accepting small residual financial risk only if that could yield upside opportunities. Value for money, affordability and long-term financial sustainability are our primary financial concerns in fulfilling our regulatory responsibilities, but we are open to considering other benefits and constraints in evaluating financial plans.

It is **essential** we remain a financially viable organisation to ensure continued public protection through continued operation. Significant financial risks are not compatible with this requirement.

People – Open (Employees and Partners)

We aim to invest in our people to create innovative mix of skills environment. We are prepared to accept risk as long as there is the potential for improved culture, recruitment and retention.

It is **essential** that risk taking in this area is consistent with the HCPC's values and culture. As an employer are committed to upholding and promoting Equality, Diversity and Inclusion.

Reform – Open (Regulatory Reform)

We support innovation, with demonstration of benefit or improvement in service delivery. We are receptive to taking difficult decisions when benefits outweigh risks. Processes, oversight and monitoring arrangements enable considered risk taking.

It is **essential** that the opportunities taken with regulatory reform are fully evidenced and cross organisational impact is considered and documented.

Data – Open (Quality, analysis, sharing)

We accept need for operational effectiveness in distribution and information sharing. We support innovation and new approaches, as long as there is the potential for improved data quality. *(Please note data protection is covered by the Compliance risk type)*

It is **essential** that we understand our data when sharing and publishing analysis.

Appendix 3 Assurance Map Pillars

Guidance and Processes	Are guidance's and processes documented, up to date (with an agreed review cycle), and accessible to all members of the department?
Training and Induction	Have all members of the department been through the appropriate corporate and department specific induction process? Have all members been trained on the processes/systems/etc required to do their job? If gaps are identified, are department members given the further training needed?
KPIs and Reporting	Is the department meeting both the council reported KPIs and department specific KPIs/SLAs? Is the work of the department regularly reported to the appropriate level, whether ELT, Committee or Council?
Quality Control	Are there quality controls in place to ensure that there is appropriate understanding and oversight of the work done by the team? This includes work trackers, quality checks, manager 1:1s, team meetings to discuss workload, QA activity, external and internal audits, etc
Continuity Planning	Is the department sustainable in terms of approach (continuous improvement) and resources (including career development, retention, recruitment and sickness) long term? This may also link to succession planning work completed with HR

Appendix 4 NAO Cyber question mapping

NAO Category	NAO Questions	Covered by ISO27001?	Covered by CE+?	Covered by NIST?	Notes & Evidence
Strategy	Is there a clear and effective cyber strategy as part of the overall business strategy, setting out the high-level actions to improve the organisation's resilience?	Y		Y	20230807 HCPC Cyber Security Strategy 2023-FINAL 20251218 HCPC Infosec PESTLE Analysis
Strategy	Are all business areas clear about their cyber security obligations and responsibilities, and resourced and empowered to implement good cyber security measures?	Y		Y	A.6.3 Annual training; 27001_2022 DOC A1 ISMS Manual v2.8b; 27001_2022 DOC A4 Management System Processes v2.10; 27001_2022 DOC A3 Effectiveness Measures v1.12
Strategy	Is sufficient funding prioritised and protected in order to match the intent of the strategy?	Y		Y	High level threats or vulnerabilities are prioritised over pure functionality enhancements to regulatory or other systems where highlighted. ISO27001 Clause 5.1 Leadership and commitment c) ensuring that the resources needed for the information security management system are available. A specific ORR risks covers lack of resources in respect of information security.
Strategy	Does the organisation understand and comply with legislative requirements, for example data protection and applicable government policies and standards?	Y		Y	A.5.31 Legal, statutory, regulatory and contractual requirements
Assurance & Oversight	Does the organisation receive regular threat briefings and assessments from NCSC and other industry partners and does this inform the risk assessment?	Y		Y	A.5.7 Threat Intelligence. Quarterly PCI:DSS scans, Internal Audit efforts from commercial auditors, Annual BSI Audits.
Assurance & Oversight	Are regular threat assessments undertaken, including representatives from across the business and the supply chain, and are unacceptable risks escalated?	Y		Y	Quarterly risk assessments are undertaken via the current Operational Risk approach, with the ability to escalate issues should they arise outside the cycle.
Assurance & Oversight	Is there regular formal reporting into the most senior decision-making body on at least a quarterly basis tracking risk tolerances and providing oversight of strategic delivery?	Y		Y	ISMS Board, now Information Security & Compliance Group, reports into Information & Technology Governance Board meetings.

NAO Category	NAO Questions	Covered by ISO27001?	Covered by CE+?	Covered by NIST?	Notes & Evidence
Assurance & Oversight	Are roles and responsibilities clearly understood?	Y		Y	A.5.3 Segregation of Duties; A.5.4 Management responsibilities. Mapped out in CIRP and in ISMS documentation
Assurance & Oversight	Does the organisation obtain assurance over the cyber security posture of critical suppliers and partners?	Y		Y	ISO27001 required for key suppliers handling information. Financial robustness monitored by Finance Dept. Also, DPIA process is imbedded within Procurement and project processes.
Assurance & Oversight	Do governance structures ensure compliance is monitored and reported effectively?	Y		Y	Annual ISO27001 BSI audits are reported to ELT & ARAC. InfoGov audits are listed in ARAC reports, results shared with asset and risk owners. Reports are discussed at ISMS Board or Information Security & Compliance Group.
Assurance & Oversight	Is the 'second line of defence' adequately resourced with sufficient expertise to provide independent challenge and oversee cyber security and resilience effectively?	Y		Y	CISRO/IG&RL sit outside IT
Assurance & Oversight	Does reporting provide meaningful insight rather than just technical detail?	Y		Y	A.5.27 Learning from information security events. High level non technical review of IIR's to ELT and ARAC
Assurance & Oversight	Does reporting explicitly link back to strategy and risk?	Y		Y	Single Strategic Cyber Security risk in new Strategic Risk Register. Maps to multiple infosec/cyber operational risks currently.
Risk Management	Have the systems, data, software, services and networks which are critical to the organisation's objectives been identified and classified by sensitivity and criticality?	Y		Y	REC 2A 20251222 RiskInfoAssets Printable A3
Risk Management	Is cyber security risk integrated into and considered as part of the overall approach to risk management and considered in strategic decision making?	Y		Y	As part of the DPIA process Cyber risks are assessed for any information linked project or deployment.
Risk Management	Is a cyber risk register in place, with clear owners, actions and escalation mechanisms?	Y		Y	Currently operates through the Operational Risk Management for Information Security & Information

NAO Category	NAO Questions	Covered by ISO27001?	Covered by CE+?	Covered by NIST?	Notes & Evidence
					Governance. Incident escalation is via CIRP & A.5.24,25,26,27,28
Risk Management	Has the organisation defined and communicated its cyber risk appetite and tolerance levels, and if so, are these integrated into decision making, investment, and mitigation plans?	Y		Y	Currently operates through the Operational Risk Management for Information Security & Information Governance; scoring all risks pre and post mitigation under Confidentiality, Integrity & Availability. This is treated at the same scale as departmental risks. These are assessed by the Information Governance function. Pure IT risks are maintained by the Head of IT. High risks are mitigated down to at least medium.
Risk Management	Is there a structured method or framework for managing risk that fits the organisation's business and technology needs, for example ISO/ IEC 27001, 27005, NCSC Cyber Assessment Framework (CAF), noting that government departments and arm's-length bodies are mandated to meet or exceed the security outcomes specified in the appropriate CAF profile (baseline or enhanced) for their critical systems?	Y		Y	ISO27001 & Cyber Essentials Plus are in use.
Risk Management	Are cyber risks regularly reviewed in line with the evolving threat landscape, and does this include those arising from newer technologies, such as developments in artificial intelligence, cloud computing and cloud-native architecture?	Y		Y	DPIA includes specific AI clauses to incorporate AI potential issues. Cloud risks are covered by A.5.23 Information Security for use of Cloud Services
Risk Management	Has the organisation gained assurance over the cyber security of its commercial partners and suppliers of products and services, including through contractual obligations, audits or certifications?	Y		Y	Suppliers handling or accessing HCPC data required to be certified to ISO27001 or Cyber Essentials Plus
People	Are board members fully aware of their responsibilities for cyber governance, and have they received appropriate training?	Y		Y	A.6.3 Information security awareness, education and training

NAO Category	NAO Questions	Covered by ISO27001?	Covered by CE+?	Covered by NIST?	Notes & Evidence
People	Does the organisation foster a positive cyber security culture, with the appropriate tone set from the top?	Y		Y	Clause 5.1. At Corporate induction a no blame but report culture is propagated, although frequent incidents from individuals would be monitored and reacted to.
People	Is there clear executive accountability for cyber security, and is this responsibility cascaded across the organisation?	Y		Y	Information Governance = Exec Dir Corp Affairs Information Technology = Exec Dir of Resources CISRO > IG&RL in future
People	Has a baseline assessment of the organisation's current cyber expertise been conducted, identifying gaps and areas of weakness?	Y		Y	Areas of expertise not included in the capabilities of internal resources, are covered by Insurers for major issues under our Cyber Security Insurance policy.
People	Is there a structured programme to ensure that all staff have at least a basic level of cyber awareness?	Y		Y	A.6.3 Annual training is mandatory
People	Is there regular evaluation of the effectiveness of cyber awareness initiatives?	Y		Y	2022 DOC A3 Effectiveness Measures v1.12. Impact of initiatives such as AI based Redaction, are evaluated periodically under the Business Change (Project) process.
People	Are third-party contractors and temporary staff included in cyber awareness and training programmes?	Y		Y	A.6.3 (PARTNERS. Council members, Temps/Contractors.)
People	Is there a plan in place to develop or obtain access to the cyber security skills and expertise the organisation needs?	Y		Y	Basic requirements for CISRO/IG&RL = ISO27001 Lead Auditor or Implementor plus Data Protection Officer Practitioner Certificate in Information Governance; other specialties within IT Dept
People	Are cyber policies developed collaboratively with relevant departments (for example, human resources) and clearly communicated across the organisation?	Y		Y	Annual review with impacted depts (A.6.= HR; A.7. = Facilities/Estates; A.8. = IT; A.5 = All operational & regulatory departments)
People	Is there a simple and trusted process for reporting cyber incidents or concerns, and a culture where staff feel confident to do so?	Y		Y	A.5.25 Assessment and decision on information security events. IIR reports with Information Risk scoring

NAO Category	NAO Questions	Covered by ISO27001?	Covered by CE+?	Covered by NIST?	Notes & Evidence
People	Does the organisation regularly reassess its resilience plans against known breaches reported by other organisations?	Y		Y	On going, but not limitless capacity, periodically attend infosec conferences on threats
Incident Planning, Response & Recovery	Does the organisation have a well-prepared and tested cyber incident response plan aligned with its risk appetite and business continuity priorities?	Y	Y	Y	A.5.24 information security incident management planning and preparation. A.5.26 Response to information security incidentsCIRP in place, and periodic tests are carried out, and incidents are responded to used as tests of the process.A.6.8 Information security event reportingA.8.16 Monitoring activities
Incident Planning, Response & Recovery	Is the plan regularly exercised for likely scenarios and updated for lessons learned?	Y		Y	BCM/DR testing approx. two dept per year, covering all major depts every three years unless incidents occur which are treated as testing in practice.
Incident Planning, Response & Recovery	Does the organisation have clarity on the sources of external support (for example, legal, technical, communications) available during a major incident, and are these integrated into the response plan?	Y		Y	A.5.26 Response to Information Security Incidents; A.5.30 ICT Readiness for business continuity.A.5.24 Information security incident management planning & preparation. CIRP
Incident Planning, Response & Recovery	Have lessons been learned from past incidents or near misses, and have they informed improvements?	Y		Y	SER (NMR) process and responses to individual IIR's; maintained in the Improvement Log
Incident Planning, Response & Recovery	Is there sufficient monitoring and logging in place to identify a potential intruder or attack, and are the warnings promptly acted upon?	Y	Y	Y	Ongoing Microsoft Sentinel use with three alert / threat levels. Monthly (approx.) reviews by CISRO/IG&RL.
Incident Planning, Response & Recovery	Is there an adequate data and asset backup strategy in place?	Y		Y	A.8.13 Information Back up (Cloud & alternate cloud for key data) Data replication within Cloud and additional version of Registration System data

NAO Category	NAO Questions	Covered by ISO27001?	Covered by CE+?	Covered by NIST?	Notes & Evidence
Incident Planning, Response & Recovery	Are controls in place to protect backups from being compromised or destroyed during an attack?	Y		Y	A.8.13 Information Back up (Cloud & alternate cloud for key data)