

Department of the Premier and Cabinet

Internal Audit

Strategic Plan: 2023-24 to 2025-26

Annual Audit Plan: 2023-2024

June 2023

Contents

1. Introduction	3
2. Service Delivery / Resourcing	4
3. Audit Planning and Assessment Approach	5
4. Strategic Audit Plan and link to DPC / OQPC Strategic Plans.....	6
5. Annual Audit Plan – 2023-24.....	6
Appendix 1 – Annual Audit Plan for 2023-24	7
Wait-list audits 2023-24	11
Appendix 2 – Prior audit activity	13

1. Introduction

This Strategic Internal Audit Plan (Strategy) and Annual Audit Plan (the Plan) sets out the scope of planned work to be undertaken by the Department of the Premier and Cabinet's (DPC's) Internal Audit Function for the financial years 2023-2024 to 2025-2026.

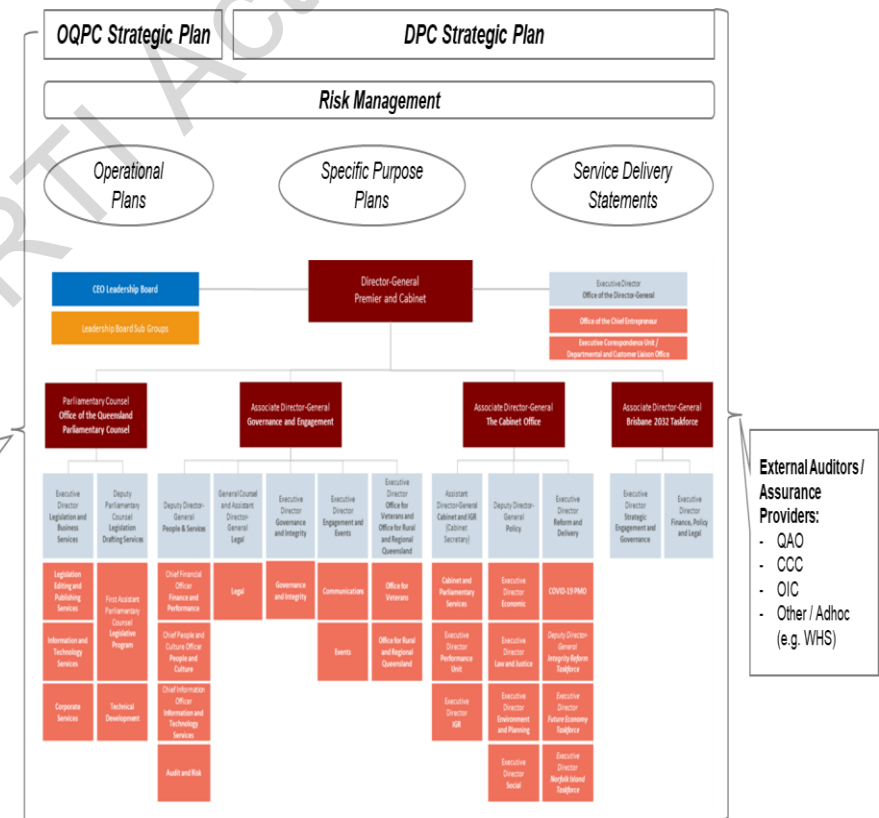
In accordance with the Internal Audit Charter, Internal Audit and Risk service (IARS) must prepare the Strategy and Plan for endorsement by the department's Audit and Risk Management Committee (ARMC), prior to final approval by the Director-General.

The Strategy and Plan has been prepared in accordance with the requirements of Internal Audit's guiding legislation: section 78(1) of the *Financial Accountability Act 2009* and section 26 of the *Financial and Performance Management Standard 2019*.

As required under the Institute of Internal Auditor's (IIA) International Standards for the Professional Practice of Internal Auditing (the Standards), the Strategy and Plan have been developed having regard to DPC's, including the Office of the Queensland Parliamentary Counsel's (OQPC's) strategic objectives and enterprise risks.

External environmental factors impacting DPC have also been considered throughout audit planning activities. Internal Audit represents a fundamental pillar in DPC's governance and assurance environment and provides a valuable means for assisting Executive Management in effectively managing risk.

IARS breadth of activity is represented in the service delivery diagram below:



2. Service Delivery / Resourcing

Internal Audit Service Delivery

Internal Audit's Charter defines the role, responsibilities, authority, and standards for Internal Audit's operations.

Internal Audit seeks to deliver value to the department through a collaborative approach and a business improvement lens aimed at highlighting opportunities for efficiency gains.

Internal Audit provides:

- Assurance that business processes and the risk and control environment are designed and operating effectively.
- Management support in an advisory capacity including process design / design of system controls, project governance, policy development, financial, operational and compliance processes.
- Leadership and supporting in promoting a culture of high ethical standards, integrity, transparency, and accountability.

DPC's Internal Audit and Risk Services (IA&RS) provides a range of advisory and assurance services including planned audit and advisory reviews, 'by request' audit and advisory services, follow up of both internal audit and Queensland Audit Office and other external assurance provider audit recommendations, together with secretariat services for the ARMC and the Finance, Performance, Planning and Risk (FPPR) Subcommittee (where requested).

IA&RS also provides services to the Public Sector Commission (PSC) under a Service Level Agreement (SLA). Priorities, budget, and resourcing for these services are scoped separately in the PSC Strategic and Annual Audit Plan 2023-24.

To maximise resourcing allocations, PSC's Plan leverages the DPC plan where possible, with at least one corporate governance related audit undertaken as part of the broader portfolio.

Internal Audit Resourcing

Internal audits identified within the Strategy and Plan are delivered through a third-party provider under a co-source partnership arrangement, currently with Ernst & Young (EY). The Director, IA&RS manages the contract, which includes an annual review of performance against key performance indicators, which is reported to the ARMC.

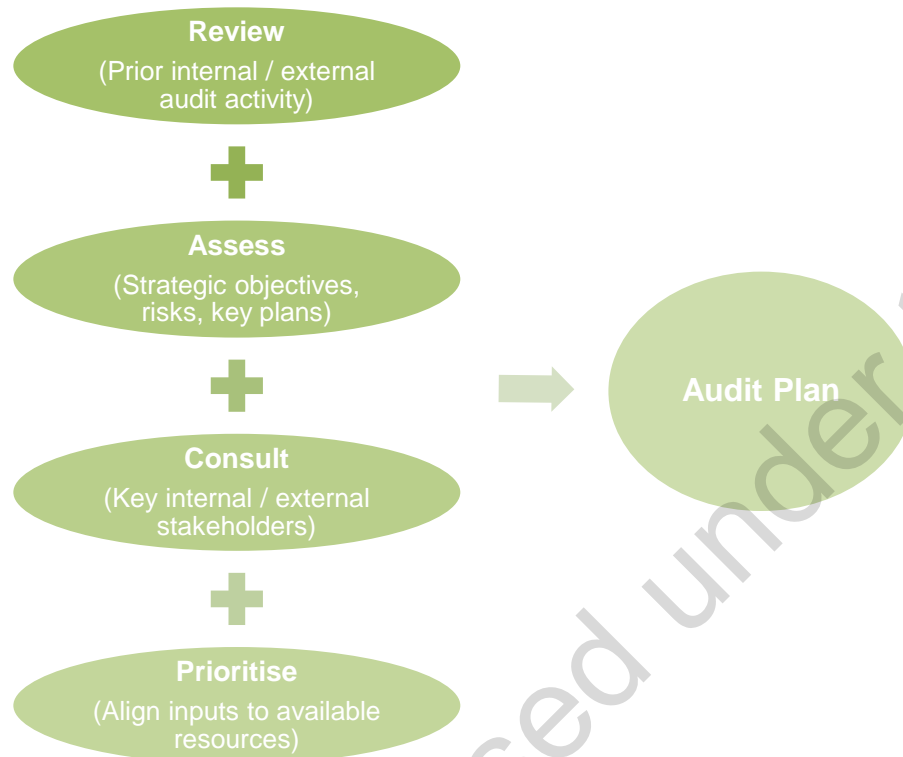
Funding for EY's services has been factored at the same level as the 2022-23 audit plan at \$252,000. This is consistent with the previous co-source provider arrangement for the period 2019 to 2022. Audit engagements have reduced to seven planned audits for the next Plan to provide greater depth of coverage.

Further reassessment of the Internal Audit resourcing will occur with broader DPC financial planning processes in preparation for the 2024-25 DPC budget.

An audit Wait-list has again been included with the Plan. This caters for prioritised audit activities originally considered for inclusion in the Plan but excluded predominantly due to resourcing constraints (refer **Appendix 1**).

3. Audit Planning and Assessment Approach

In developing the individual audit assignments for the Strategy and Plan, Internal Audit and Risk Services (IARS) has applied a risk-based approach has been applied, including consideration of input areas both internal and external to DPC. The diagram below depicts the high-level approach to development of the Plan:



The input areas covered under the audit planning approach IA&RS followed in assessing and prioritising individual audits for the Strategy and Plan are detailed in the table below:

Input	Summary of work performed
Enterprise and divisional risk registers	Risk registers were reviewed as a part of planning processes. Key auditable areas for the identified risks were assessed.
Previous internal audit activity	Internal audit findings from previous activities were considered as a part of planning processes.
Corporate information	DPC's Strategic Plan and other operational plans such as Strategic Workforce Plan.
Global, National, and State trends	Each quarter IA&RS conducts an environmental scan for the FPPR and the ARMC. The scan is based on audit reports tabled at the state and federal levels, and other publications of interest.
Other forms of assurance (QAO, CCC)	Other forms of assurance were considered as part of planning, including findings identified from: <ul style="list-style-type: none"> • previous QAO financial and performance audits and the focus of upcoming performance audits • the Crime and Corruption Commission (CCC) • the Queensland Information Commissioner.
Key stakeholder consultations	Input was sought from key stakeholders to ascertain key and emerging areas of risk, strategic priorities, major changes, programs, and projects.

4. Strategic Audit Plan and link to DPC / OQPC Strategic Plans

In preparing the Strategy and Plan, IARS has directly considered DPC's and OQPC's strategic direction, with alignment of audit activities directly linked to the *Strategic Plan 2023-2027* (drafts) per the below table:

Strategic Plan Area	Audit Topic	2023-24	2024-25	2025-26
Policy Leadership	Path to Treaty Readiness Assessment		X	
	Norfolk Island Governance Oversight			X
	The Cabinet Office Knowledge Hub / Data Repository			X
Communication and Engagement Management (DPC) / Strategic Engagement with Partners (OQPC)	Stakeholder Management	X		
	Events Management		X	
Strong Accountable Government	Ministerial Expenses		X	
	Core Internal Controls (Ministerial Services)			X
Lead Brisbane 2032 Olympic and Paralympic Games	Brisbane 2032 Coordination Office – Governance Health Check	X		
	Brisbane 2032 Coordination Office – Performance Assessment (in advance of two-year review)		X	
A High-Performing Workforce (DPC) / A Skilled, Flexible, and Resilient Workforce (OQPC)	Recruitment and Selection Processes	X		
	Staff Lifecycle Management (Onboarding and Offboarding)			X
	Succession Planning (including Managing Critical personnel risk)		X	
A High-Performing Workforce (DPC) / Strategic Engagement with Partners (OQPC)	Cyber and Data Breach Response and Readiness	X		
	Contract Management Over Key Contracts	X		
A High-Performing Workforce (DPC) / A Healthy and Inclusive Workplace (OQPC)	Psychosocial Risk Management			X

Strategic Plan Area	Audit Topic	2023-24	2024-25	2025-26
A High-Performing Workforce (DPC)	Business Continuity Planning	X		
	Implementation of Queensland Protective Security Framework	X		
	Business Critical ICT Controls			X
	Grants Management			X
	Information Management Governance Framework		X	
	Identity and Access Management		X	
	Third Party Risk Management			X
Stewardship of Innovation and Change (OQPC)	Legislation Accessibility		X	

5. Annual Audit Plan – 2023-24

The list of audits proposed for the 2023-24 Plan has been prioritised on based on the following criteria:

- Identified risks (predominantly the revised Enterprise Risks agreed by the Executive Leadership Team in April 2023). Further divisional level risks may be considered during detailed audit scoping.
- Frequency of audit presence and historical audit activity within the suggested review area (internal or external audit).
- Specific requests suggested by the business.

The full Plan is provided at **Appendix 1** (pages seven to ten) below. A Wait list is also provided (per pages eleven to twelve) catering for audit activity originally considered for inclusion in the Plan but excluded due to resourcing and prioritisation constraints.

Prior years' internal audit activity is outlined in **Appendix 2**.

Appendix 1 – Annual Audit Plan for 2023-24

The following table outlines the proposed Annual Audit Plan for DPC for financial year 2023-24 based on current risks and business priorities. This Plan will be assessed throughout the year as business priorities change and in line with reporting requirements to the ARMC. The audit scopes below are indicative at the time of Plan development and may change to meet operational needs once detailed scoping occurs. Each audit activity is referenced to a corresponding DPC Enterprise Risk (ER).

Review Type	Audit Title	Audit Description	Alignment to Enterprise Risks (ER)	Approx. Timing	Approx. Days
Communication and Engagement Leadership (DPC); Strategic Engagement with Partners (OQPC)					
Advisory	Stakeholder Management Audit Sponsor: <i>Executive Director, Office of the Director-General</i>	Internal Audit will assess department-wide processes for engaging and communicating with key stakeholders at both departmental and whole-of-government levels. The audit activity will include: <ul style="list-style-type: none"> reviewing processes for stakeholder identification, including influence, interest, needs and expectations evaluating stakeholder engagement activities, feedback mechanisms, (including the DPC Customer Survey) and relevant communication channels identification and mapping of responsibility for whole of government communications within DPC (e.g., leadership of regular whole of government communications versus whole-of-government crisis communications) assessing processes for managing stakeholders, aligning with DPC's goals and objectives and reporting and monitoring activities. <p><i>Consideration will be given to OQPC elements being mapped separately during the detailed scoping phase.</i></p>	ER #6 Ineffective engagement of stakeholders and customers, including regional communities in Queensland, resulting in misaligned plans impacting implementation of the government's objectives for the community.	Q2	30

Review Type	Audit Title	Audit Description	Alignment to Enterprise Risks (ER)	Approx. Timing	Approx. Days
Lead Brisbane 2032 Olympic and Paralympic Games					
Advisory	Brisbane 2032 Coordination Office – Governance Health Check Audit Sponsor: CEO Brisbane 2032 Coordination Office	Internal audit will assess the governance approach deployed within the Brisbane 2032 Coordination Office to manage the portfolio of programs across Queensland Government for the 2032 Olympic and Paralympic Games. The audit may include assessment of: <ul style="list-style-type: none"> • risk identification, documentation, and management • scope management, reporting, oversight, and escalation processes • governance structure to enable effective decision-making • internal and external stakeholder management. 	ER #8 Ineffective program planning, development, implementation, and oversight constrains timely delivery of key Departmental priorities.	Q1	20
A High Performing Workforce (DPC); A Skilled, Flexible, and Resilient Workforce (OQPC)					
Assurance	Recruitment and Selection Processes Audit Sponsor: Associate Director-General, Governance & Engagement	Internal Audit will assess the design adequacy, operating effectiveness, and consistency of application of key business processes for the recruitment and selection of departmental employees. The audit will include: <ul style="list-style-type: none"> • compliance with existing processes • management of conflicts of interest • screening activities. <i>Internal Audit coverage will also consider targeted recruitment strategies such as the Aboriginal and Torres Strait Islander Recruitment Strategy.</i>	ER #3 Inability to attract, retain and optimise an appropriately qualified and skilled workforce hindering the Department's provision of high-quality service delivery.	Q2-Q3	22

Review Type	Audit Title	Audit Description	Alignment to Enterprise Risks (ER)	Approx. Timing	Approx. Days
<i>A High Performing Workforce (DPC); Strategic Engagement with Partners (OQPC)</i>					
Assurance	Cyber and Data Breach Response and Readiness <i>Audit Sponsor:</i> <i>Chief Information Officer</i>	Internal audit will assess the DPC's incident response capability including: <ul style="list-style-type: none"> • response to digital asset threats • capability to prevent, detect, mitigate, and respond to ransomware incidents. This audit will also consider the Information Services Unit's processes to perform adequate and sufficient levels of cyber due diligence across third party services.	ER #1 Breach of information assets through inadvertent or malicious activity, impacting people, information, and assets, leading to significant business disruption, information loss and /or data or privacy breach.	Q3	28
Assurance	Contract Management Over Key Contracts <i>Audit Sponsor:</i> <i>All Divisional Leads</i>	Internal audit will undertake an end-to-end assessment of the department's contract management practices, including: <ul style="list-style-type: none"> • contract creation, execution, and registration • compliance with terms and conditions, including management of contract variations • risk management and assessing supplier performance • managing finalisation and/or renewal of contracts • contract reporting and data management • education activities provided to contract owners/managers. <i>Reports will be generated at Divisional level, with a wrap up / summary report provided to the Director-General.</i>	ER #7 Poorly designed and implemented corporate governance processes, resulting in a breach of compliance obligations, inefficient decision-making or impacts to integrity and transparency.	Q3-Q4	24

Review Type	Audit Title	Audit Description	Alignment to Enterprise Risks (ER)	Approx. Timing	Approx. Days
A High Performing Workforce (DPC)					
Assurance	Business Continuity Planning (DPC Framework and relationship to WoG Framework) Audit Sponsor: <i>Associate Director-General, Governance & Engagement</i> <i>Associate Director-General, The Cabinet Office</i>	<p>Internal Audit will assess the implementation of the department's Business Continuity Framework and relevant activities, including planning, reporting, monitoring, and alignment to contemporary resilience practice.</p> <p>The audit will include assessment of departmental processes for management whole-of government requirements and flow-on impacts to the department's resilience practices.</p> <p><i>Audit fieldwork will be department-wide, with consideration given to Divisional-level reporting to assist in uplift of individual business area's Business Continuity Plans.</i></p>	ER #4 Inability to effectively respond to or recover from disasters, environmental impacts or pandemics resulting in prolonged business interruption.	Q1-Q2	26
Assurance	Implementation of Queensland Protective Security Framework Audit Sponsor: <i>Chief Security Officer</i>	<p>Internal audit will assess activity progressed across the department for the implementation of the Queensland Protective Security Framework to ensure compliance with the intent of the four pillars of Framework.</p> <p><i>This audit will inform activity for the preparation of the first official QPSF Attestation (due July 2024).</i></p>	ER #1 Breach of information assets through inadvertent or malicious activity, impacting people, information, and assets, leading to significant business disruption, information loss and /or data or privacy breach.	Q4	16
Other Audit Activity					
	Contingency Allocation	In preparing the Plan, IARS has retained a contingency allocation of 10 days to enable response to emerging advice requests or for further audit activity within planned audits.			
	Recommendation follow-up	IA&RS routinely follow up audit activity to ensure management implement agreed recommendation actions.			
	EY Attendance at ARMC	With the ARMC being a joint DPC and PSC Committee, DPC is allocated a proportionate cost of the co-source partner's attendance at meetings to discuss DPC audit activity.			

Wait-list audits 2023-24

In preparing the Plan, some prioritised audits originally considered for inclusion have been excluded, predominantly due to resourcing constraints. These audits will be further assessed throughout the year during quarterly review processes, or otherwise utilised as substitute audits where scheduled audits are unable to proceed due to business priority changes.

Review Type	Audit Title	Audit Description	Alignment to Enterprise Risks (ER)	Approx. Days
Assurance	Legislation Accessibility	<p>The Queensland legislation website is currently reviewed around 220,000 times per week by around 59,000 unique users.</p> <p>Internal audit will evaluate the Queensland legislation website accessibility and design of alternative text to assess processes to monitor compliance obligations according to the Web Content Accessibility Guidelines (WACG), with the aim of fostering an inclusive digital environment for all Queenslanders.</p> <p>As part of the audit, an evaluation of alternative text for images will be performed and an assessment conducted to identify any gaps between the WCAG 2.0 and 2.1 standards.</p>	<p>ER #9</p> <p>Information technology systems stability, availability and performance does not meet the needs of the Department due to ineffective governance, planning, resourcing, and change practices.</p>	22
Advisory	Core Internal Controls Processes	Following from the 2022-23 Core Internal Controls assessment (focused on HR and PSC controls), this activity will continue control assessments for DPC Finance including consideration of automation.	<p>ER #7</p> <p>Poorly designed and implemented corporate governance processes, resulting in a breach of compliance obligations, inefficient decision-making or impacts to integrity and transparency.</p>	20
Advisory	Events Management	Internal Audit will assess the design and operating effectiveness of governance and logistics arrangements to enable successful delivery of DPC scheduled Events.	<p>ER #6</p> <p>Ineffective engagement of stakeholders and customers, including regional communities in Queensland, resulting in misaligned plans impacting implementation of the government's objectives for the community.</p>	20

Review Type	Audit Title	Audit Description	Alignment to Enterprise Risks (ER)	Approx. Days
Assurance	Corporate Policy Framework	<p>The department's Corporate Policy Framework outlines the policy / procedure documents governing departmental operations and provides structure for ensuring consistency in policy and procedure development and management.</p> <p>Internal Audit will assess the design and effectiveness of the department's Corporate Policy Framework, including consideration of policy / procedure lifecycle processes (including clarity of roles, responsibilities, and accountabilities at each stage of the lifecycle).</p>	<p>ER #7</p> <p>Poorly designed and implemented corporate governance processes, resulting in a breach of compliance obligations, inefficient decision-making, or impacts.</p>	22
Assurance	IT Operations and Resilience	<p>Internal audit will assess management's ability to monitor and report on the performance of essential business services, together with the ability to remain within impact tolerance limits.</p> <p>The scope will cover the extent to which the department monitors and embeds ownership of operational resilience frameworks within the "First Line" of business, as well as link from a process and technology perspective to general controls (e.g., change management, business continuity planning and risk management).</p>	<p>ER #9</p> <p>Information technology systems stability, availability and performance does not meet the needs of the Department due to ineffective governance, planning, resourcing, and change practices.</p>	22

Appendix 2 – Prior audit activity

Division / Business Area	Review Type	Audit Title	2020-21	2021-22	2022-23
Governance and Engagement	Assurance	Core Internal Control Processes – Portable and Attractive Items	X		
	Advisory	Core Internal Control Processes – Controls Roadmap (HR and PSC focus)			X
	Assurance	Appointments and Constitutional Services Processes – Right to Information		X	
	Assurance	Conflicts of Interest (including PSC fieldwork)			
	Assurance	General Computer Controls – Ministerial Services Penetration Testing		X	
	Assurance	Ministerial Services	X	X	X
	Advisory	Performance Management Framework		X	
	Assurance	Fraud Management		X	
	Assurance	Procurement and Contract Management	X		
	Assurance	Regional Community Forum Governance			X
	Advisory	Strategic Workforce Planning			X
	Assurance	DPC Incoming Sponsorships			X
	Assurance	Compliance Management	X		
	Assurance	Information Security Management System (including ASD Essential 8)	X		
	Assurance	Media Monitoring	X		
	Assurance	Design Services	X		
	Assurance	Taskforce Governance (e.g., Commissions of Enquiry)			X
	Assurance	Event Sponsorship Fund		X	
	Assurance	Risk Management Framework	X		
Department wide	Assurance	Handling Personal Information [^]			X
	Assurance	Cyber Resilience Simulation Testing Exercise		X	
The Cabinet Office	Assurance	The Cabinet Office – Critical System Review – Cab Bag Application			X
	Assurance	Intergovernmental Relations		X	
Office of the Queensland Parliamentary Counsel	Assurance	Queensland Integrated Legislation Lifecycle System (QuILLS) – Penetration Testing		X	

[^]This audit replaced audits on General Computer Controls and Cyber Resilience Exercise Follow-up.