Internal Audit Plan 2023-24

Reviewed by Audit and Risk Committee: 22 May 2023
Reviewed by Executive Leadership Team: 30 May 2023
Approved by Acting Director-General: 23 June 2023
Endorsed by Audit and Risk Committee: 29 August 2023
Approved by Acting Director-General: 15 September 2023

Queensland Government

Document control options

Departmental approvals

Refer to the appropriate Risk Assessment Tool for relevant reviewer and approver

Date	Name	Position	Action required *(Review/endorse/approve)*	Due
11 May 2023	Samara Dowling	Acting Chief Auditor	Submission to the Audit and Risk Committee for feedback	22 May 2023
15 May 2023	Samara Dowling	Acting Chief Auditor	Development for submission to ELT	15 May 2023
30 May 2023	Samara Dowling	Acting Chief Auditor	Reviewed and endorsed by the Executive Leadership Team	30 May 2023
23 June 2023	Sally Stannard	Acting Director-General	Approved by Acting Director-General	23 June 2023
24 July 2023	Samara Dowling	Acting Chief Auditor	Updated plan to include the Customer and Digital Group (CDG)	31 July 2023
24 July 2023	Samara Dowling	Acting Chief Auditor	Reviewed and endorsed by the CDG Leadership Team	31 July 2023
29 August 2023	Samara Dowling	Acting Chief Auditor	Endorse the updated Plan for CDG by the Audit and Risk Committee	29 August 2023
15 September 2023	Sally Stannard	Acting Director-General	Approved by Acting Director-General	15 September 2023

Contents

1. Executive Summary

Overview

In accordance with s31 of the *Financial and Performance Standard 2009* (FPMS), an Internal Audit Plan (the Plan) has been developed to provide the **Director-General** with independent assurance over identified risk exposures of the Department of Transport and Main Roads (TMR) for the period 1 July 2023 to 30 June 2024.

Under Section 61 of the *Financial Accountability Act 2009*, accountable officers have a responsibility to ensure the operations of the department are carried out efficiently, effectively, and economically, and are to establish and maintain systems of internal controls.

The intent of this document is to outline the proposed internal audit work plan for the 2023-24 financial year. The document also examines, at an overview level, the expected risks and challenges for Department of Transport and Main Roads, and how this will influence annual internal audit work plans, including potential internal audit topics/ themes beyond the 2023-24 year. The 2023-24 internal audit plan will be reviewed during the year to ensure that it remains relevant and current. The Plan may be amended during the year if and as required. Amendments to the plan will be communicated to the Audit and Risk Committee (ARC).

Role of Internal Audit

Internal Audit provides an independent and objective assurance function to the Director-General. It is a requirement of the Internal Audit Charter that the Head of Internal Audit prepares an internal audit annual work plan for the consideration of the TMR ARC. The TMR ARC Charter states that the committee has responsibility to review the proposed internal audit plan to ensure it covers key risks and that there is appropriate co-ordination with external audit.

Internal Audit's Objectives

Internal Audit's objectives as per the 2022-2025 three-year Strategic Internal Audit Plan are to:

1. Provide contemporary assurance services that assist TMR to better manage its risks and deliver its business objectives and strategic priorities.
2. Have assurance systems and processes enabling operational efficiency to meet stakeholder expectations.
3. Engage stakeholders to embed a customer service focus to better understand, plan and respond to TMR needs.

Internal Audit provides an objective review and advisory service to:

- Deliver objective insights on risks, controls, assurance and compliance outcomes throughout TMR.
- Provide assurance to the Senior Leadership Team and the ARC that TMR's operational and financial controls are designed to manage the organisation's risks and are operating in an efficient, effective and ethical manner.
- Bring external expertise, innovation and perspectives to assist TMR in achieving its objectives and enhance its performance.
- Support the ARC in acquitting its role and responsibilities.

Internal Audit's assurance activities will complement departmental monitoring practices and oversight from external regulators and central agencies to provide the Director-General with confidence that an internal control framework is operating efficiently and effectively over key financial, compliance, operational and reporting processes in accordance with the *Financial Accountability Act 2009*.

2. Approach to developing the 2023-24 Internal Audit Plan

The Plan Development Process

The Plan has been developed through consultation with the department's senior executives, leadership groups, external ARC members, external audit – Queensland Audit Office (QAO) and Internal Audit analysis of the department's strategic objectives, operational and risk documents and other relevant documents from across the public and private sectors.

Consultative Approach

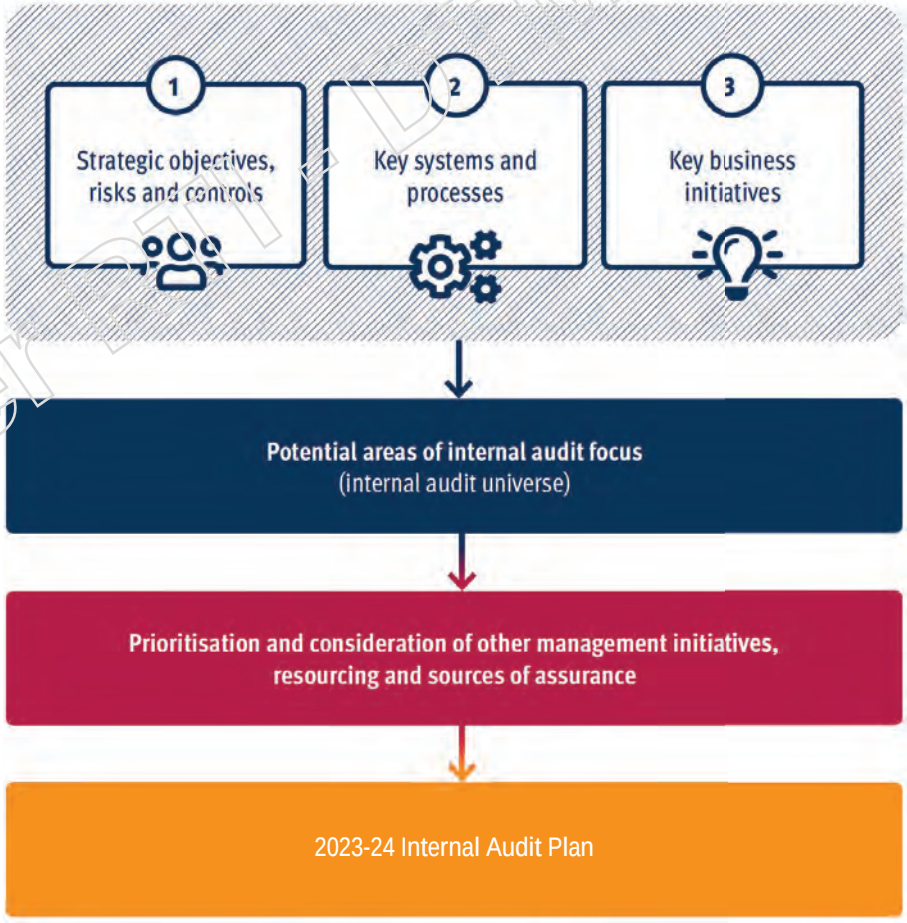
The Plan has been developed to identify an appropriate coverage of the key risks and critical business processes and systems of TMR and give focus to current business initiatives and operational challenges. As part of the planning process, we met with key stakeholders to identify their priorities, challenges and key risks for 2023-24. The consolidation of the outcomes from the stakeholder meetings enabled us to prioritise potential reviews that could be conducted.

IA Planning Process

IA considered a range of information in developing the Plan including:

- risk artefacts highlighting prevalent strategic and operations risks
- business planning documentation and initiatives
- new internal audit thought leadership, industry and regulatory developments
- major initiatives, programs and projects
- financial statements and fraud risks
- media reports
- previous internal audit activity and the key findings and themes identified from our work.

The above factors were incorporated into the development of the Plan and the **active watch/ reserve list** at **Appendix A**. The active watch/ reserve list provides alternative reviews which could be incorporated into the Plan through the unallocated component based on emerging risks or trends.



3. Internal Audit Resources

Capacity and availability of resources to deliver Internal Audit Services

- The budget includes resources of **1500 delivery days** allocated for TMR internal audit reviews to be delivered by inhouse internal staff and co-source external providers. **1050 delivery days have been allocated to specific reviews.**
- 10% (**150 delivery days**) of the budget has been left unallocated to enable internal audit to perform value-adding advisory services.
- 20% (**300 delivery days**) of the budget has been left unallocated to enable Internal Audit to pivot and respond to management requests or major advisory requests in response to emerging risks and priorities across the department throughout the financial year.
- For the Customer and Digital Group, recently added to the TMR portfolio through the Machinery of Government changes in May 2023, the budgeted resources are approximately **280 delivery days** to be delivered by inhouse internal staff and co-source external providers. This will be broken up similarly as follows:
    - **200 delivery days have been allocated to specific internal audits** and core assurance, including management of co-source providers.
    - 10% (**30 delivery days**) has been left unallocated to enable internal audit to perform value-adding advisory services.
    - 20% (**50 delivery days**) has been left unallocated for management requests or major advisory requests in response to emerging risks and priorities.
- Any additional independent assurance can be delivered by Internal Audit throughout the year on a fee-for-service basis.
- Internal Audit understands that an internal audit approach must be flexible. While a high-level objective has been developed for each proposed review, detailed scoping discussions will be undertaken with respective business 'review sponsors', prior to commencement of internal audit review work.

Core assurance Services

Internal Audit provides 'Core Assurance' services across the department including:

- the TMR ARC Secretariat
- a Head of Internal Audit role (as mandated by legislation)
- ongoing strategic advisory support across the department (Head of Internal Audit and Director, Audit Services)
- monitoring of 2023-24 Internal Audit Plan delivery
- development of 2024-25 Internal Audit Plan
- liaison with QAO
- audit recommendation monitoring
- management reporting
- general assurance advisory and support
- advisory and observer roles on boards, working groups, committees
- robust contract management of outsourced providers.

4. Plan on a page – proposed assurance coverage 2023-24 by division

Division	Q1	Q2	Q3	Q4
Whole of Department	• ICT Assurance Map • Olympics preparedness	• Psychosocial hazards • Managing consultants and contractors	• Fraud risk in procurement of minor works • Complaints management	Asbestos Management
Customer Services, Safety and Regulation	Vulnerable customers support	MSQ Grants Management	• Monitoring effectiveness of road safety community education programs • See complaints management above	MSQ Pilotage Regime
Translink	Digital Licence project health-check	Fare evasion analysis and reporting	• See complaints management above • See fraud risk in procurement of minor works above	
Infrastructure Management and Delivery	• Delivering key infrastructure projects (risks and controls) • Asset management data lifecycle	• Security of desirable assets • Managing risk transfer in infrastructure projects	Sustainability for major projects	WHS remote and isolated work
Policy, Planning and Investment	Delivery and management of structures deferred maintenance program	Property revenue management	CSA Program support for property management	Climate Change Response Health-check
Corporate	• Supplier onboarding due diligence • Fraud risk workshops and documentation	Management of Cyber and Data Security Enterprise Operating Risks	Payroll data analytics and EBA compliance	• Queensland Procurement Policy roll-out and compliance • Accessible communications guidelines
	Behavioural Drivers and Cultural Assurance – targeted internal audit reviews			
	Source to Pay -- post implementation process and controls testing (SOD tools) – Q2/Q3			
Customer and Digital Group (CDG)	Customer and Digital Group Branch Risk Assurance Maps	Business continuity planning and disaster recovery (CITEC)	Queensland Online information privacy	
All	• **350 days unallocated for management-initiated requests** (50 for CDG) • **180 days unallocated for advisory work** (30 for CDG)			

5. 2023-24 Internal Audit Plan

The following summarises the proposed 2023-24 Internal Audit Plan. An active watch/ reserve list of internal audits is provided at **Appendix A** which may be considered as substitutes or additions to the Plan based on feedback provided from management or the Audit and Risk Committee throughout the year. The active watch/ reserve list does not incorporate a complete Internal Audit Universe, instead it is focused on those risk areas with immediate potential relevance. This approach is consistent with current industry thinking to move toward short term plans that are highly flexible to meet changing organisational needs.

A tentative forward three-year program of work has also been provided at **Appendix B**.

A schedule of previous internal audit activity from 2018-19 to 2022-23 can be found at **Appendix C**.

Internal audits have been mapped to the current departmental and enterprise operating enterprise risks at defined in **Appendix D.**

Internal Audit understands that an internal audit approach must be flexible. While a high-level objective has been developed for each proposed internal audit, detailed scoping discussions will be undertaken with respective business 'review sponsors', prior to commencement of internal audit work.

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
All	All	SR10	Olympics Games preparedness	For this internal audit, we propose a rolling program of work leading up to 2032 Olympic Games delivery. Potential internal audits include: • Governance structures, roles and responsibilities. • Accessibility planning, local government integration. • Precinct and service interfaces for traffic planning. • Contribution to meeting specific games delivery commitments, e.g. green games. • PT integration and operations.	Q1	40
All	All	SR17 EOR749 EOR750	ICT Assurance Map	TMR adopts a federated model for ICT planning support and delivery. This provides a level of complexity when determining an overarching plan to obtain assurances over the risk management and controls across ICT services owned by TMR. The purpose of this audit is to develop an assurance map for key ICT systems across TMR in order to understand the risks and controls in place, governance processes and the levels of assurance over the performance of these controls. This will include	Q1	40

[1] Strategic Risk and Enterprise Operational Risk are detailed in **Appendix D**

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
				an assessment of TMR's capability to protect itself against cyber incidents for ICT systems. It is proposed that internal audit will review a rolling program of ICT systems, including ITB managed systems, locally managed systems in divisions or branches and may also include other entities accessing TMR systems.		
All	All	SR11	Managing consultants and contractors	TMR utilises contract and consulting services to facilitate delivery of critical services, either to supplement workforce or to provide specialist advice or opinions. This internal audit will look at processes to engage, report, monitor, maintain knowledge and analyse the use of consultants and contractors across TMR in accordance with policies, procedures and any whole of government requirements or guidance.	Q2	30
All	All	EOR906	Psychosocial hazards management	The Managing the risk of psychosocial hazards at work Code of Practice 2022 is a practical guide on how to prevent harm from psychosocial hazards at work, including psychological and physical harm. The Code is an approved code of practice under the Work Health and Safety Act 2011. It provides information for persons conducting a business or undertaking (PCBU) on how psychosocial hazards and risks can be controlled or managed and can be used to help decide what's reasonably practicable to reduce risk. The release of the Managing the risk of psychosocial hazards at work Code of Practice 2022 (the Code) along with amendments to the Work Health and Safety Regulation, are important steps in keeping Queensland workplaces safe, healthy and productive. This internal audit will look at how TMR has implemented the new requirements under the code as well as the changes to the Work Health and Safety Regulation, and how compliance is being evidenced.	Q2	30
TransLink CSSR Corporate	TransLink CSB Governance	SR10	Complaints management	Effective complaints management can help organisations to retain customers, enhance their reputation, and identify areas of improvement. It is therefore important for organisations to have clear policies and procedures in place to manage complaints effectively. This internal audit will look to ensure that TMR has sound processes in place to ensure that complaints received across the department are consistently and accurately captured, analysed, investigated, resolved and reported. This scope will include complaints received through the different mediums and from the different sources (divisions/ branches) across TMR.	Q3	40

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
All	All	EOR807	Fraud risk and procurement for minor works	Internal Audit conducted a survey across the TMR leadership team (Director and above) in 2022 to identify where the perceived areas of greatest inherent and residual risk existed with respect to fraud within the department. The results of this survey indicated that areas with respect to third parties (procurement, vendor selection, tendering and probity) along with data security were perceived to be the areas of greatest risk. As a result, in 2022, internal audit performed a fraud risk framework and a deep dive activity over procurement and third-party fraud risk, focussing on major capital infrastructure projects. In 2023, ICAC performed an investigation into awarding of Roads and Traffic Authority and Roads and Maritime Services contracts in return for benefits and found fraud occurred throughout each of the planning, sourcing and managing phases of the procurement process for minor works. This internal audit will look at the risk of procurement fraud, bribery and corruption risk across minor works and procurement activities, ensuring that the controls in place to prevent fraud are designed and operating effectively	Q3	40
Corporate CSSR	Finance Facilities CSB	EOR906	Asbestos Management	This internal audit will review processes and controls in place to manage asbestos in TMR owned or leased premises (including existing properties, those managed by EPW, and future state properties) from an employee workplace health and safety perspective.	Q4	30
CSSR	CSB LTSR	SR10	Vulnerable customers support processes	In provision of services to the public, the public sector, including TMR, has a responsibility to ensure that all customers, including those in vulnerable categories (for example, those with financial hardship, or those living in rural and remote communities), are able to utilise services, including concessions, licences and identity documents. From the customer's perspective, select a sample of TMR customer support services and assess the processes and policies in place to support equality of service and inclusivity in accessing those services.	Q1	30
CSSR	MSQ	SR20	MSQ Grants Management	Assess the adequacy, effectiveness and efficiency of grants processes, including systems, policies, controls, justification of decision making and reporting on acquittal for grant approvals for grants.	Q2	30

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
CSSR	LTSR	SR10	Monitoring effectiveness of road safety community education programs	The purpose of road safety initiatives is to drive positive change in Queensland's road use culture through community engagement and education campaigns, focusing on high risk behaviour and vulnerable road users, as well as working with other jurisdictions to ensure consistent road safety messaging. This internal audit objective is to look at investment prioritisation decisions, campaign approval processes, campaign creative process and the evaluation of campaign effectiveness.	Q3	30
CSSR	MSQ	SR14	MSQ Pilotage regime	This internal audit objective is to look at the Maritime Safety Queensland (MSQ) Pilotage Regime, including the controls around the processes for ensuring adequate licencing, assessments of skills, delivery of contract requirements including KPIs and other agreed performance management actions, for example fatigue management controls for pilotage services.	Q4	40
TransLink	PTS	SR21	Digital Licence Expanded project health-check	Perform a program/project health check on the reporting, governance, time and cost, budget, project lifecycle, security and privacy, scenario testing, escalation and cybersecurity aspects of this project.	Q1	30
TransLink	PTS	SR20	Fare evasion analysis and reporting	TransLink has undergone a series of interventions to reduce the impact of fare evasion. The purpose of this internal audit is to test the impact of programs invested in to reduce fare evasion, including the roll-out of SNOs and interactions with the Queensland Police Service, as well as the reporting on such.	Q2	30
IMD	PDO	SR10	Delivering key infrastructure projects (risks and controls)	Assess the design and operation of processes and controls to identify, assess and manage infrastructure project delivery risks across PDO. This review will include consideration of project risk management activities and project financial management processes.	Q1	30
IMD	RoadTek	SR19	Asset management data lifecycle	RoadTek are contracted to maintain road assets (for example, line markings, structures, guardrails) on behalf of TMR under an agreement with the PDO branch. The objective of this internal audit is to look at the efficiency and accuracy of processes and systems in place to capture and report on asset management activities (including asset maintenance) over an asset's lifecycle, including creation, maintenance and disposal, to inform future asset investment decisions.	Q1	30

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
IMD	All	EOR807	Security of desirable assets	The objective of this internal audit is to check the adequacy of processes and controls in place to prevent the theft of desirable assets, like equipment and valuable commodities like fuel and copper.	Q2	30
IMD	PDO	SR14 SR16 SR21	Managing Risk Transfer in Infrastructure Projects	The objective of this internal audit is to check the processes and controls in place to ensure that risk transfer (for example, public utility plant and contaminated land) in projects (including identifying, managing, and transferring risks to infrastructure projects) is adequately managed when planning works, that contracts are appropriately set up to manage risk transfer and that learnings from projects are incorporated into the Transport Infrastructure Project Delivery System for future projects.	Q2	40
IMD	PDO	EOR822	Sustainability for major projects	The Queensland Government requires all government infrastructure projects over $100 million to have a sustainability assessment completed. The Infrastructure Sustainability Council of Australia's (ISCA) Infrastructure Sustainability Rating Scheme is an approved method to achieve this objective, assessing and driving sustainability in infrastructure. TMR has committed to undertaking formal IS assessments for projects over $100M in order to drive environmental, social and economic outcomes. The purpose of this internal audit is to assess processes in place to measure cost, value and impacts of initiatives during the design, construction and operation of infrastructure assets to achieve sustainability (resources and associated carbon) outcomes in major projects.	Q3	40
IMD	PDO RoadTek	EOR906	WHS remote and isolated work	TMR has a requirement under workplace health and safety legislation to manage the health and safety risks to remote or isolated workers, and have systems in place to effectively communicate with workers The purpose of this internal audit is to check compliance with workplace health and safety requirements for remote and isolated work, as well as assess the controls in place to mitigate risks around remote and isolated work.	Q4	30
PPI	PIP	SR20	Delivery and management of structures deferred maintenance program	The objective is to assess the effectiveness and efficiency of the process for prioritisation, development of the works program, delivery, and performance reporting for Structures (Element 19).	Q1	40

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
PPI	GP	SR10	Transport Academic Partnership financial statement certification	Transport Academic Partnership (TAP) is a collaboration between the Department of Transport and Main Roads (TMR), the Motor Accident Insurance Commission (MAIC), Queensland University of Technology, Griffith University, and the University of Queensland. This advisory work is to check the financial statements are supported by the agreement	Q1	10
PPI	SPM	EOR807	Property revenue management	The purpose of this internal audit is to test the processes in place to review, renegotiate, collect and report on rental/ lease revenue for commercial and residential properties owned and managed by TMR.	Q2	30
PPI	SPM	EOR807	Control Self-Assessment program property management	Review the Control Self-Assessment (CSA) Framework to ensure that it identifies issues and potential exposures to achieving strategic objectives, effectively evaluates the controls in place to manage risks and provides appropriate assurance to support effective management decision making.	Q3	30
PPI	TP	EOR822	Climate change response actions	TMR's climate change response actions and strategies are aimed at mitigating and adapting to the impacts of climate change in Queensland. For the transport sector, and as part of the initiatives include to reduce greenhouse gas emissions, vehicle emissions, adapt and be resilient to climate change risk (including natural disasters) to aid delivery a single integrated transport network accessible to everyone. The objective of this internal audit is to check processes in place to measure monitor and report on commitments under the Climate Change and Resilience Strategy.	Q4	30
PPI	TSP	EOR4	Transurban Data Risk and Quality Review	Assess Transurban's internal controls and compliance with the Tolling Capability Agreement for security administration practices, facilities, risk management and quality assurance practices.	Q4	10
Corporate	F&P	SR15 EOR807	Supplier onboarding due diligence	Check the process to assess potential vendors and contractors into categories of risk prior to performing a suite of controls to check that vendors are who we want to engage with, from a human rights, fraud, bribery and corruption, anti-terrorism perspectives. Checking into who owns the companies, any connection with criminals, and checking that companies we buy from aren't linked to employees or anyone committing fraud.	Q1	40
Corporate	Gov	EOR807	Fraud risk workshops and documentation	Performance of fraud risk workshops across selected branches to assist in understanding and documenting localised fraud risks and mitigating controls.	Q1	10

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
Corporate	ITB	SR17 EOR749 EOR750	Management of Cyber and Data Security Enterprise Operating Risks	The Chief Information Officer is the responsible officer for a number of controls and treatments that mitigate strategic and enterprise wide operating risks, as well as being the owner of two enterprise wide operating risks with respect to ICT. This internal audit objective is to assess the approach to the management of the Enterprise Operating Risk for ITB to ensure that the right level of controls is in place to provide adequate assurance to responsible officers that the control environment for key systems is adequately managed.	Q2	40
Corporate	F&P HRB	EOR807	Payroll Data Analytics and EBA compliance	Using data analytics, perform a series of tests to look for anomalies in payroll data, assessing assurance provided by QSS, and compliance with payroll policies, procedures and Enterprise Bargaining Agreement (EBA) terms and conditions.	Q3	40
Corporate	F&P	SR11 SR15	Queensland Procurement Policy Compliance	Check readiness for compliance with the updated Queensland Procurement Policy (QPP), including the application of best practice principles (including Best Practice Industry Conditions (BPICs)) for major projects.	Q4	30
Corporate	GOV	SR10	Accessible Communications Compliance Accessible Transport Network (ATN) Project	In order to provide accessible communications to Queenslanders as well as all staff at TMR, a project has commenced in order to provide more accessible communications. This internal audit will look at the project scope, timetable, reporting and monitoring comparing it to legislation, standards and better practice.	Q4	30
Corporate	F&P	SR15	Source to Pay – post implementation process and controls testing (SOD tools)	Ensure the controls designed and implemented in the new Source to Pay (S2P) system adequately address the risks inherent in the process. Confirm vendors are being managed appropriately in the new system. Provide ongoing support for changes arising as TMR goes live with source to pay solutions.	Q2/Q3	40
Corporate	All	VARIOUS	Behavioural Drivers and Cultural Assurance – targeted assurance	Determine the strength of the behavioural controls that support the department's control environment. Internal Audit could perform: • Root Cause analysis - behavioural or cultural reasons for control weaknesses • Deep Dives into specific process areas to understand behavioural control strengths, weaknesses and develop targeted solutions to improve the behavioural drivers (culture) • Departmental / system-wide assessments of the strength/ weakness of behavioural controls with respect to the Code of Conduct, or other relevant policies	All	30

Division	Branch	Risk #[1]	Internal audit title	Scope description	Timing	Days
Customer and Digital Group	All	VARIOUS	Customer and Digital Group Risk Assurance Maps	Develop an assurance map for key processes within branches and significant units/ teams across the Customer and Digital Group in order to understand the risks and controls in place, governance processes and the levels of assurance over the performance of these controls. It is proposed that internal audit will review a rolling program of key processes across branches and significant units/ teams, the deliverable for which will be a Risk Assurance Map that can be handed back to the relevant executive for maintenance	All	90
Customer and Digital Group	Transformation and Enabling Technologies	SR17 EOR750	Business continuity planning and disaster recovery (CITEC)	Assess the design adequacy and operating effectiveness of business continuity planning and disaster recovery controls for CITEC, including management's testing of plans, and the incorporation of lessons learned and better practices following disruptive events. Consider the impact on Agencies utilising the full suite of services provided by CITEC.	Q2	40
Customer and Digital Group	Service Delivery and Operations	EOR1050	Queensland Online information privacy	Assess the design and operating effectiveness of controls to address key privacy risks for the handling and management of Personally Identifiable Information (PII) and sensitive information.	Q3	40
All	All	VARIOUS	Management Initiated Requests	To respond to emerging risks and priorities throughout the year – allocation at the request of management with prioritisation determined by the Chief Auditor.	All	300
All	All	VARIOUS	Advisory Work	Management may request Internal Audit to provide assurance advisory services that may require specific days to be allocated. This service differs from traditional internal audit engagements and may involve advisory work around governance, risk management and control matters.	All	150

Appendix A: Active watch/ reserve list

While the internal audits in the watch list below are currently considered lower priority than those in the Plan, Internal Audit acknowledges that with the dynamic nature of risk, priorities can change. Should any changes to the risk profile or any emerging risks arise, the Plan remains flexible and can adjust accordingly with the consultation of the Audit and Risk Committee. If the reviews are not undertaken in 2023-24, they will be considered in future internal audit plans if they still remain a priority.

- Human rights
- Instruments of delegation
- Strategic risk deep dive
- Whistle-blower process and compliance
- CSB procurement practices
- Body worn cameras (MSQ/ CSB)
- Vessel Safety Management System
- Infringement notices
- Registration process
- Motor vehicle inspection centres
- Customer refunds
- Written-off vehicle inspections - contract management
- CSB technical governance
- MSQ management of boat ramp & marine infrastructure
- Contract management and ICT governance (CSB)
- Rollingstock ETCS alliance arrangement
- Transport services contract
- Major projects delivery Logan and Gold Coast faster rail, Beerburrum to Nambour rail upgrade
- Demand responsive transport implementation blueprint
- Bus network reinvestment plan
- Project management maturity assessment
- Contractor safety management (managing infrastructure risk)
- Project and program information management
- Asbestos management for structures (RoadTek)
- RoadTek performance reporting on project and program process improvement review
- Federal/ commonwealth funding process
- Property disposals
- Environmental risk management
- Zero emissions vehicle strategy
- Development of the Queensland Road System Performance Plan (QRSPP)
- TMR Asset Management Plan - asset investment analysis
- Prioritisation of ICT investment
- WHS Safety Management System (ISO45001)
- Cyber/ data security response framework
- Service delivery model (HRB)
- WHS responsible officer due diligence
- TMR Integrity Framework – Coaldrake Review
- TMR governance structures framework and efficacy
- Data storage and backups
- Forward procurement
- Procurement risk assurance map
- Information management strategy
- Media management processes
- Risk management training & capability
- CDG ICT Systems Lifecycle Planning
- CDG ICT Risk Assurance Maps
- Fraud risk in shared services accounts payable
- CDG Program delivery and management
- Privacy and security of information captured through the Camera Detected Offence Program

Appendix B: Three-year indicative internal audit topics

The three-year indicative internal audit topics provides an indication of proposed reviews in future years based on stakeholder discussions for the development of the 2023-24 Internal Audit Plan. The items in the active watch/ reserve list in **Appendix A** have not been included in the annual plan for 2023-24. This is only an indication of potential review and given the dynamic nature of risk and changing departmental priorities, a full consultation process will be undertaken each year for the development of each year's final Internal Audit Plan as outlined in Section 2 of this document.

Based on the current resources, Internal Audit allocates between 25-30 reviews in the annual program of work so the three-year indicative list assumes Internal Audit will continue its core assurance work, specifically its advisory involvement in key digital governance projects and initiatives including Source2Pay and Smart Ticketing. Internal Audit will continue its development of data analytics across key areas through its Continuous Controls Monitoring initiative.

Division	YEAR 1 – 2023-24	YEAR 2 – 2024-25	YEAR 3 – 2025-26
Cross Department	As above	• ICT Assurance Maps • Human rights • Instruments of delegation • Strategic risk deep dive • Whistle-blower process and compliance	• ICT Assurance Maps • Privacy compliance • Induction processes • Business planning • Implementation of TMR Accessibility and Inclusion Action Plan
Customer Services, Safety and Regulation	As above	• CSB procurement practices • Body worn cameras (MSQ/ CSB) • Vessel Safety Management System • Infringement notices • Registration process • Motor vehicle inspection centres • Customer refunds • Written-off vehicle inspections - contract management • CSB technical governance • MSQ management of boat ramp & marine infrastructure • Contract management and ICT governance (CSB)	• Tow truck scheme • Approved inspection station scheme • Online services customer experience • Digital product strategy • Business exceptions • PCI-DSS compliance • Boat harbour operations • Procurement practices • Pollution response incident reviews

Division	YEAR 1 – 2023-24	YEAR 2 – 2024-25	YEAR 3 – 2025-26
TransLink	As above	• Major projects delivery –Logan and Gold Coast faster rail • Rollingstock ETCS alliance arrangement • Transport services contract • Demand responsive transport implementation blueprint • Bus network reinvestment plan • Ticketing equipment management contract	• Major projects delivery –Beerburrum to Nambour rail upgrade • Strategic Rail – risk and control mapping • Safety and security assessments • Ticketing and tracking on school services (TAT's) project • TransLink's digital future's program trialling innovative digital proofs of concept • Concession cards • Personalised transport reform • Financial sustainability & operational excellence project • Safety and security assessments
Infrastructure Management and Delivery	As above	• Asbestos management for structures (RoadTek) • RoadTek Respect Action Plan • TMR crash investigation policy • Next generation traffic signalling project • Regional infrastructure contract management optimisation • Project management maturity assessment • Contractor safety management (managing infrastructure risk) • Project and program information management • RoadTek performance reporting on project and program process improvement review • SNO CSA program	• PDO response to disruptive events • RoadTek - Delivery program office capability and benefits realisation review • Olympics preparedness, Operations and PT integration • Cooperative and Automated Vehicle Initiative • Safety at roadworks sites • Natural disaster relief and recovery arrangements • Control Self-Assessment data automation • Worksite safety practices for contractors
Policy, Planning and Investment	As above	• Federal / commonwealth funding process • Property disposals • Environmental risk management • Zero emissions vehicle strategy • Development of the Queensland Road System Performance Plan (QRSPP) • TMR Asset Management Plan - asset investment analysis	• Transport network pricing (revenue sustainability) • QTRIP – change request/ variation management • Assurance map and CSA program • corridor preservation, management & investment • Property contractor engagement & management – data analytics

Division	YEAR 1 – 2023-24	YEAR 2 – 2024-25	YEAR 3 – 2025-26
Corporate	As above	• Corporate Performance Management Transformation Project • Cyber and data security risk • Prioritisation of ICT investment • WHS Safety Management System (ISO45001) • Cyber/ data security response framework • Service delivery model (HR) • WHS responsible officer due diligence • TMR Integrity Framework – Coaldrake Review • TMR governance structures framework and efficacy • Data storage and backups • Forward procurement • Procurement risk assurance map • Information management strategy • Media management processes • Risk management training & capability	• ICT Portfolio, Programme and Project assurance • Data storage and backups • Software asset management framework • Digital capability • SAP HANA controls support • Data protection & data privacy • Discipline / suspension processes • Delegation management • WHS incident management and reporting • ITB software asset management framework • ITB digital capability
Customer and Digital Group	As above	• ICT Systems Lifecycle Planning • ICT Risk Assurance Maps • Fraud risk in shared services accounts payable • Program delivery and management • Privacy and security of information captured through the Camera Detected Offence Program	• ICT Risk Assurance Maps • Fraud risk in shared services payroll • Corporate Administration Agency Risk Assurance Map

Appendix C: Previous Internal Audit Activity

Division	2022-23	2021-22	2020-21	2019-20
Cross Department	• Staff recruitment and retention strategies • TMR premises physical security • Supply chain cyber incident preparedness • MaaS implementation roadmap actions • TMR Indigenous strategy • ESG Mat	• Rehabilitation services • Fraud and corruption risk and control assessments • Controls design and optimisation	• Mandatory staff training • Management of excess leave • BCP lessons learnt • Covid risk and control assessment • Governance of business-led ICT projects • Source 2 Pay - controls consultation	• Privacy framework • ICT federated governance • Employee performance management • Flexible work arrangements • Business continuity and disaster recovery • Strategic risk control and treatment validation review • Conflicts of interest • Fraud risk control validation
Customer Services, Safety and Regulation	• Regulatory performance LTSR • Regulatory performance CSB • LTSR grants and subsidies management • CSB safety hazard inspections • MSQ Asset Management • MSQ WHS risk assessments/ management • Optus Data Breach response	• Customer service branch continuous improvement project • Prosecution services • MSQ assurance map • MSQ compliance effectiveness regime • MSQ flood response to SEQ rainfall and flood event	• MSQ COVID-19 foreign crew changeover process • Accountable stock • MSQ foreign crew changeover – review #2 • MSQ foreign crew changeover – review #3 • CSB CSA automation review • Transport inspection regime • LTSR/MSQ CSA framework • TRAILS Internal Controls – Third Party Access • MSQ Foreign Crew Change Over – Review #4 • Governance over SSQ Agreement	• CSA framework – CSB • Digital Wallet gate 3 project assurance review • Regulatory decision-making – traffic controller accreditation • Review of vehicle duty collections • Regulatory decision-making – heavy vehicle access

Division	2022-23	2021-22	2020-21	2019-20
TransLink	• Accessible access to public transport network • Smart Ticketing project health-check • Concept timetables • TransLink incident management and reporting • Taxi subsidy scheme continuous controls monitoring • Regulatory performance	• Rail governance and interfaces • TransLink control self-assessment program (regional operations) • TransLink performance management framework and dashboards • Disposal of taxi restricted use slips process	• Legislative compliance framework • Transport services contracts • Legislative compliance – TransLink • Senior Network Officers deployment • Covid-19 financial management of relief packages – essential services • Smart ticketing health check • NGR third-party contractor WHS management	• Assurance map – TransLink • Smart Ticketing assurance plan and initial 'health-check'
Infrastructure Management and Delivery	• Collaborative contracting • Corridor protection	• RoadTek contractor and subcontractor management • Traffic data collection and use • Traffic data integrity and security • RoadTek legislative compliance • RoadTek emergency response planning and management	• RoadTek timesheets and allowances • Program and project assurance Framework – PDO • Minor equipment asset Management – RoadTek • BMTMC governance review	• Assurance map – RoadTek • Assurance map – PDO • Construction materials testing • Quarry registration scheme • ETCS payment process review • CSA framework - PDO • Project management maturity assessment – RoadTek
Policy, Planning and Investment	• Property and land resumptions • Long-term infrastructure investment planning • Transport academic partnership governance health-check • Property management and maintenance	• Infrastructure risk management • Early acquisitions of TMR property and land • Transurban Queensland bypass tolling capability agreement	• 3PCM optimisation follow up review • Backlog management - surfacing treatments and pavement rehabilitation	• State boat harbours financial controls and governance arrangements • MT Isa line incentive scheme

Division	2022-23	2021-22	2020-21	2019-20
	• Transurban data risk and quality review	• Delivery and management of surfacing treatments • Performance data integrity – transport analysis	• Transurban tolling capability agreement – Toowoomba bypass • Covid-19 financial management of relief packages – rent relief	• Review of prioritisation of transport infrastructure investments • Review of benefit management within the transport infrastructure portfolio
Corporate	• Fraud risk data analytics over procurement spend • Source to Pay controls support • Behavioural Drivers roll out • Legal services process mapping • Relationship Access Manager (RAM) access and control • Employee attraction and retention strategies	• Succession management • Policy and procedures framework • Facilities management – capital works • Source to Pay SAP Ariba wave 1 controls • Source to Pay SAP Ariba wave 1 user access testing – phase 1 • Source to Pay SAP Ariba wave 1 controls – phase 2 • Cloud governance and security • Legal services contract management • WHS framework rollout and compliance • Corporate cardholder financial delegation accreditation • Overseas travel process follow-up • Winshuttle governance framework review	• CFO assurance statement framework • ISMS maturity health check • Use of staff replacement & specialised contractors • Cyber security incident management • Cape/ case management • Information management recordkeeping solution • Financial delegation management	• Transurban security audit • Toowoomba second range crossing toll revenue management process • WHS assurance framework • strategic ICT risk and control treatment validation • TRAILS financial internal controls • Fleet management
Other	• GCWA regulatory compliance	• DPC ISMS review		

Division	2022-23	2021-22	2020-21	2019-20
Cross former CHDE Department that included CDG	• Community recovery Ready Reserve payroll management	• Information security (Essential 8) • Service delivery arrangements • ICT Governance	• Financial and contract delegations	
Customer and Digital Group	• SSQ Concessions Payments • Workforce planning recruitment and retention -SSQ	• Business continuity planning and disaster recovery: ServiceNow • Data Privacy • Customer and stakeholder engagement		• Contract management

Appendix D: Strategic and enterprise operational risks

Below is a list of strategic and enterprise operational risks as contained in TMR's Risk Management System in March 2023.

	STRATEGIC RISKS
SR10	Failure to provide safe, accessible and integrated transport solutions to meet customer needs and resilience requirements.
SR11	The skills, capabilities and agility of our workforce does not deliver TMR's strategic objectives and future transport system.
SR12	Inability to appropriately plan for and respond to a transport network and service delivery disruption.
SR14	Lack of effective partnerships in rail to deliver a safe, sustainable and integrated transport system.
SR15	Contract management and procurement processes, practices and capabilities are not fit for purpose to deliver expected outcomes and value for money for the State and TMR.
SR16	The capacity, capability and maturity of the supplier market does not support TMR's future transport service priorities and ability to deliver capital projects on time and on budget.
SR17	Unsustainable ICT systems and protection against cyber threats
SR19	TMR does not maximise the value from data it processes for planning and operational purposes.
SR20	Inability to fund and sustain essential transport network development, systems, operations, management and services.
SR21	Non-delivery of critical projects at a departmental and transport portfolio level (e.g. electoral/political commitments).
SR1050	Unable to deliver future ETCS deployment packages required by the Rail Network Strategy (RNS)
EOR822	Failure to meet TMR's environmental and climate change obligations and commitments in accordance with legislative requirements, government and internal policies, and community expectations
EOR1050	Information is not governed and managed to meet TMR's obligations, derive value and deliver on our services.
EOR807	There is a risk TMR may be vulnerable or exposed to fraud and corruption due to weaknesses within the internal and external control environment.
EOR749	Failure to prevent the unplanned degradation of TMR's critical ICT assets, including infrastructure.
EOR750	Failure to protect TMR's critical ICT assets, including on-line services, from unauthorised access, misuse, and malicious cyber security attacks.
EOR906	Failure to ensure the health and safety of workers and others in the workplace