B. Audit scope and methods

Performance engagement

This audit has been performed in accordance with the *Auditor-General Auditing Standards*, incorporating, where relevant, the standards on assurance engagements issued by the Auditing and Assurance Standards Board. This includes the Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. This standard establishes mandatory requirements, and provides explanatory guidance for undertaking and reporting on performance engagements.

Audit objective and scope

The objective of the audit was to assess public sector entities' preparedness to respond to and recover from cyber security incidents.

The audit addressed the objectives through the following sub-objectives and criteria:

Sub-objective 1:	**To evaluate the effectiveness of strategies and guidance supporting the management and coordination of cyber security response and recovery capabilities across state and local government.**
Criteria 1.1	Lead agencies establish strategies and procedures that enable and support entities to effectively manage and coordinate cyber security response and recovery capabilities.
Sub-objective 2:	**To evaluate selected entities' level of preparedness to respond to and recover from cyber security incidents.**
Criteria 2.1	Entities develop, implement, and maintain risk-based strategies and plans to effectively identify and respond to cyber security incidents.
Criteria 2.2	Entities can effectively isolate cyber security incidents to restore capabilities or services that were impaired, capturing lessons learnt through reporting.

The entities we audited

The entities subject to this audit included:

- the Department of Transport and Main Roads, specifically the Cyber Security Unit (formerly within the Department of Communities, Housing and Digital Economy) – is responsible for setting cyber security policy and guidance for Queensland Government departments and statutory bodies, and providing assistance to government owned corporations and local governments
- the Department of Housing, Local Government, Planning and Public Works (Local Government was formerly within the Department of State Development, Infrastructure, Local Government and Planning) – regulates the local government sector, including councils' corporate governance, and administers the local government legislation and the sector's funding program. It aims to build council capability and grow a positive council culture of strong, accountable decision-making and financial management.

We also audited 3 public sector entities (state and local government entities). We do not want to compromise the security of these 3 entities by publicly identifying their security vulnerabilities, so we have not named them in this report.

We acknowledge the 3 entities have different levels of resourcing and capability for managing cyber security risks. We use the term 'entities' in this report to refer broadly to all Queensland public sector entities (departments, statutory bodies, and government owned corporations) and local governments.

Exclusions from the scope of the audit

As part of the audit, we did not:

- assess prevention of cyber security incidents
- undertake exhaustive technical analysis on the adequacy of detailed processes used to detect and respond to cyber incidents
- assess the quality of technical advice provided to entities in the event of an incident.

Audit methods and approach

The audit was conducted from May 2023 to January 2024 and consisted of:

- field interviews and site visits
- documentation analysis
- data analysis
- cyber security simulations led by our subject matter experts.

Field interviews and site visits

We conducted interviews with key officials, staff, and stakeholders from:

- the Department of Transport and Main Roads, specifically the Cyber Security Unit (formerly within the Department of Communities, Housing and Digital Economy)
- the Department of Housing, Local Government, Planning and Public Works (Local Government was formerly within the Department of State Development, Infrastructure, Local Government and Planning)
- 3 additional public sector entities.

Document review

We obtained and reviewed relevant documents from the entities involved in the audit. This included legislation, strategic plans, annual plans, guidelines, correspondence, performance reports, reviews, and evaluations. We also considered research from other jurisdictions and academia.

Data analysis

We analysed data from:

- the Cyber Security Unit's training attendance records
- audited entities' incident reporting systems.

Subject matter experts

We engaged a team of subject matter experts in cyber incident response to assist in the audit. The team provided advice to the Queensland Audit Office on the assessment of entities' strategies and plans against better practice frameworks. The team also conducted cyber security simulations, which assessed:

- technical skillsets, capabilities, and capacities for detecting, containing, and eradicating cyber incidents
- responses to a complex cyber incident, including communication and escalation of decision-making
- recovery from, reporting, and learning from an adverse event.