B. Performance engagement

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

The conclusions in our report provide reasonable assurance that the objectives of our audit have been achieved. Our objectives and criteria are set out below.

Audit objective and scope

This audit examined whether entities effectively manage their cyber security risks.

It addressed this by assessing whether entities:

- understand and assess to what extent their information assets and organisational processes are exposed to cyber security risks
- design and implement effective information controls to mitigate identified cyber security risks.

Scope exclusions

We did not, as part of this audit, examine the effectiveness of activities conducted by the Queensland Government Chief Information Office. Only one of the three entities in this audit use the services of the Queensland Government Chief Information Office.

Entities subject to this audit

We selected three entities for this audit. We have not named the three entities in this report as we do not want to compromise their security by publicly identifying their security vulnerabilities.

We provided each of the in-scope entities with a detailed report on the risks we identified through our detailed testing, specific to their entity.

We acknowledge the three entities have different levels of resourcing and capability for managing cyber security risks.

Audit approach

We conducted the audit in accordance with the Auditor-General of Queensland Auditing Standards—September 2012, which incorporate the requirements of standards issued by the Australian Auditing and Assurance Standards Board.

The audit included:

- interviews with staff from the three in-scope entities
- review of documents and analysis of data
- a red team assessment for each of the three entities. A red team engagement tries to find the quickest method to access an entity's security mechanisms and compromise its sensitive applications and data. In doing so, it considers the target and resources available, and may attempt social engineering, physical entry, and data exploitation
- an open source threat intelligence assessment to determine whether any sensitive information about the three entities could be obtained from public sources
- testing whether the entities had implemented the 'Top 4' of the 'Essential Eight' mitigation strategies published by the Australian Cyber Security Centre to help organisations protect their systems against cyber threats
- interviews with staff from the Queensland Government Chief Information Office (as a stakeholder).