E. Using third-party assurance reports

Assurance reports enable governance and reduce waste

Entities remain accountable for their financial statements and the security of their information, even when a third party hosts their system or holds their data. Without an assurance report, entities have no independent evidence that the provider's controls work. The third party is audited once, and distributes the report to many of its customers, therefore reducing effort and costs for government services.

External auditors also need evidence that controls at service providers operate effectively. Assurance reports are the main way to obtain this evidence. When reports are missing, incomplete, or late, audits take longer and the auditor often has to complete alternate procedures. This means the entity pays its auditor to do work it has already paid the service provider to cover often leading to delays and additional costs.

Reports and certificates do not all provide the same assurance

ASAE 3402 reports are the base standard for financial reporting

ASAE 3402 reports cover a service provider's controls relevant to its customers' financial reporting. The service provider describes its controls. An independent auditor tests them and gives and opinion on them.

The Auditing and Assurance Standards Board issues Standard on Assurance Engagements ASAE 3402 *(Assurance Reports on Controls at a Service Organisation).* ISAE 3402 is the international equivalent, and System and Organization Controls 1 (SOC 1) is the United States equivalent. They are nearly identical. In practice, they serve the same purpose, and external auditors rely on them equally.

A Type 1 report covers whether controls are properly designed at a point in time. A Type 2 report also covers whether the controls operated effectively over a period, typically 6 months or 12 months. Auditors generally need a Type 2 report.

These reports are not public. Providers give them to their customers and their customers' auditors, usually when a contract requires it. They also often exclude the provider's own service providers; this is called a carve-out. For example, a report may exclude the data centre that physically hosts a system, even though the contract with the third party includes hosting services. The data centre controls are then not covered by the auditor's opinion.

SOC 2 reports cover security, not financial reporting

System and Organization Controls 2 (SOC 2) reports cover a provider's controls over security, availability, processing integrity, confidentiality, and privacy. They are useful for overseeing cyber security risks but are not designed for financial audit reliance. Many providers offer both SOC 1 and SOC 2 reports; they have some overlap but serve different purposes.

Certificates are not replacements for assurance reports

Certifications such as ISO 27001, which covers information security management systems, confirm that a provider's management system meets a standard at a point in time. A certificate does not describe the provider's individual controls, does not report the results of testing them, and does not give an opinion on whether they operated effectively over a period.

Certificates are a useful signal of a provider's security practices, but entities cannot rely on them in place of an assurance report. Auditors do not rely on these documents. Figure E1 provides an overview of the types of third-party reports used by entities.

Figure E1
Types of third-party reports

Report	What it covers	What it is useful for
ASAE3402 Type 2 (or ISAE 3402 / SOC1)	Controls relevant to customers' financial reporting, tested over a period	Third-party risk management Reliance by external auditors
SOC2	Controls over security, availability, processing, integrity, confidentiality, and privacy	Overseeing cyber security risks
Certificates (like ISO 27001)	Confirms a management system meets a standard's requirements at a point in time	A signal of the provider's practices at a point in time. Not a substitute for an assurance report.

Source: Queensland Audit Office.



Assurance reports and certifications are not interchangeable. Entities should match the report to the risk, system, control objective, and period it needs assurance over.

Entities need to obtain and review assurance reports

Entities can typically only obtain assurance reports if their contracts specify them.

Management should:

- when negotiating a contract – require the service provider to deliver an annual assurance report and specify the standard to be used (for example, ASAE 3402 Type 2), the scope, the period it must cover, and when the entity will receive it. Entities should obtain the assurance report, not just be given access to view it
- when renegotiating or renewing a contract – add an assurance report requirement if the current contract does not include it. Renewal is often the only practical opportunity to address this gap
- every year – obtain the assurance report and the check the period it covers aligns with the entity's financial year. Where there is a gap between the end of the report period and the end of the financial year, obtain a bridging letter from the provider or a Type I report at the period end date.

Management should review each report as part of good third-party risk management and governance. Management should check and document:

- whether the auditor is independent and reputable
- whether the scope covers the systems used by the entity
- scope exclusions (including carve-outs) and whether they need a separate report
- the auditor's opinion, including any qualifications
- exceptions found in testing, if any, and whether they affect the entity
- complementary user entity controls – these are controls the report assumes the entity performs itself, and the entity should confirm it performs them.

Entities should receive and review assurance reports in time for the auditor to review them, well ahead of when the financial statements are to be certified. Late reports delay the audit.