Third Party Technology Assurance Reporting

Organisations are more dependent than ever on third parties to fulfil their critical business processes across their value chain. Coupled with rapid digitisation, this means that **organisations are increasingly outsourcing their technology solutions**.

Outsourcing technology controls and data handling **does not outsource the risk**. As such, there is a need for transparency over the controls in place within third parties to ensure that they are suitably robust and in line with the risk profile of the services and data held. **Regulatory scrutiny** is increasing, requiring more direct oversight by Management and the Board on third party matters of risk management and ongoing due diligence. Additionally, **third party incidents and customer service disruptions are increasing**, often with immediate public visibility, and greater severity of customer, reputational, regulatory and financial consequences.

To **build trust and win in the marketplace**, technology service providers should demonstrate strong risk management and internal control practices over the services they provide. A third party assurance report provides service organisations a 'ticket to play' in their ecosystem. It signals to the market they are serious about risk management, and have received independent assurance that their internal controls are effective.

SOC 2 is a framework which has become the standard for service organisations to report on the effectiveness of non-financial controls, particularly among technology service providers. Awareness of SOC 2 has grown considerably in recent times and organisations outsourcing their technology solutions are increasingly requesting a SOC 2 report as part of contracting (re)negotiations. **A SOC 2 report is fast becoming a licence to operate**.

SOC 2

The System and Organisation Control 2 (SOC 2) framework includes five 'Trust Services Criteria' ("TSCs"):

- Security
- Availability
- Confidentiality
- Processing Integrity
- Privacy

Security is mandatory for any SOC 2 report and other TSCs can be scoped in based on the services that an organisation provides and the associated risks. Each TSC includes a set of requirements / objectives, to which an organisation maps their controls. These controls are then audited and a SOC 2 report is prepared under an assurance standard, allowing the report to be shared with a service organisation's customers or prospective customers, thus providing transparency and building trust. Additional frameworks (e.g., ISO 27000, NIST) can be built into a SOC 2 report to create a 'SOC 2+'. The format of a SOC 2 report is as follows:

Independent service auditor's report *- This is a short form letter which describes the scope and responsibilities of each party, limitations and assurance opinion on control effectiveness.*

Management's assertion *- A signed assertion from management that the representations made to the auditor during the audit were complete and accurate and that management have met their responsibilities.*

Description of the system *- A description of the overall system of control related to the in-scope areas. Content coverage is prescribed by the SOC 2 framework and includes infrastructure, software, people, procedures and data. This section can be a useful marketing tool and provides a reader with detailed insight into a service organisation's control environment.*

Information provided by the service auditor except description of controls *- The description of control activities to meet the SOC 2 TSC(s), with the tests performed and the outcome of those tests.*

Why should you partner with Deloitte?

We have a dedicated team of SOC 2 and third party assurance experts.

We have extensive third party assurance experience with small, medium and large organisations.

We use a proven approach/methodology that is scalable to organisations of all sizes.

We can mobilise global teams of specialists to meet your reporting requirements and deadlines.

We are recognised for our independence, objectivity and pragmatism.

Benefits of a SOC 2 report

Competitive advantage: A SOC 2 report is a key enabler when attracting and retaining business and is often a requirement of RFPs

Operational disruptions: Eliminate multiple audits by business partners and customers that require valuable time and resources of operational and service personnel

Improve organisational risk governance: An assurance journey which identifies control gaps, allowing you to focus investment on remediation and fostering a culture of improvement

Meeting client compliance requirements: Helping clients satisfy their regulatory requirements, particularly as it pertains to data management

Stakeholder risks: Address growing concerns among executive management, audit committees and board members about availability and security risks

Ally MacLeod
Partner
Tel: 0404 070 896
Email: amacleod@deloitte.com.au