JANUARY 2023

SOC 2+: ENHANCING YOUR EXISTING CONTROLS ASSURANCE REPORTING

IS YOUR ORGANISATION GETTING THE MOST OUT OF THEIR INFORMATION SECURITY COMPLIANCE EFFORTS?

OPTIMISING YOUR COMPLIANCE EFFORTS AND REPORTING TO GAIN A COMPETITIVE EDGE

In a world overflowing with cyber threats, customers and partners want to be assured that their service providers are on top of the latest cyber security and privacy related risks. That's why it's critical for these service providers to demonstrate their commitment to protecting data, mitigating risk, and staying ahead of industry trends and changes to meet their customer's expectations.

Obtaining a SOC 2 report establishes trust, which is critical to your bottom line, and it can be a competitive differentiator when closing new business.

Most organisations are familiar with SOC 2, a minimum-security requirement for Service Organisations providing a managed service or processing and/or storing customer data in the cloud. It focuses on securing and protecting customer data across five categories called Trust Services Criteria (TSC).

However, many organisations are unaware of the enhanced SOC 2+ option that assures compliance beyond the five TSC's. It includes multiple regulatory and industry frameworks such as the National Institute of Standards and Technology (NIST) and the International Standardization Organisation (ISO).

SOC 2+ reports are rapidly gaining popularity as they address different risks and industry specific regulations

Third party assurance reporting based on the TSC is not sufficient for some service providers due to additional industry-specific regulations and requirements. For this reason, more service providers start to adopt an integrated SOC 2+ approach that incorporates multiple frameworks and industry standards into third party assurance reporting for greater coverage of potential risks.

This extensible framework creates significant benefits for both user organisations and service providers, as it is based on a common control framework and also addresses a broad range of industry control requirements reducing the amount of resources for third party oversight.

Health Information Trust Alliance (HITRUST) — the framework supports standards that are required at all stages of transmission and storage of health care information to help ensure integrity and confidentiality

International Organisation for Standardisation (ISO) 27001 — the international standard for securing information assets from threats and provides requirements for broader information security management

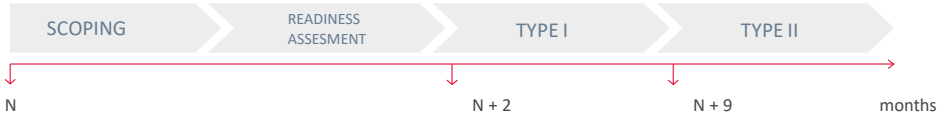
Cloud Security Alliance (CSA) — CSA, in collaboration with the AICPA, developed a third-party assessment programme of cloud providers officially known as CSA Security Trust & Assurance Registry (STAR) Attestation

National Institute of Standards and Technology (NIST) — the NIST framework focuses on improving cybersecurity for critical infrastructure

Emerging and evolving frameworks and regulations - as the world around us changes, regulations and compliance frameworks are created or adapted to respond to those changing needs. SOC 2+ can accommodate these needs and integrate relevant aspects of Privacy regulations (e.g. GDPR), Sustainability (e.g. CSRD), Cyber legislations (e.g. Cybersecurity act), etc.

How BDO Can Help

We know that keeping up with various compliance requirements can be demanding, especially if you don't know where to start. That's why our advisors are uniquely equipped to meet you wherever you are on your compliance journey and to help you become more proficient in your approach to third-party reporting. BDO has the necessary expertise and track record in advising service providers throughout the entire attestation process, applying a pragmatic and risk-based approach enables an organisation to obtain Type 2 attestation in a minimum of 9 months (depending on scope, complexity and maturity).



For more information on the benefits of TPA for cybersecurity and other key organisational issues, see our recent paper, Third Party Attestation—a Strategic and Systematic Approach to Managing Risks. For a tailored approach on how you can improve your organisation's approach to cybersecurity, please contact Sam Khoury or Christophe Daems.

Sam Khoury
Partner, Third Party Assurance
BDO in Canada
skhoury@bdo.ca

Christophe Daems
Partner, Global TPA Community leader, BDO in Belgium
christophe.daems@bdo.be