

ARTICLE

The SOC compliance connection

Achieving your compliance requirements

Massive data breaches continue to make headlines, and organizations are taking note. For many, each new breach of privacy is a worrying reminder that ineffective data protection programs can cause irreversible reputational damage. In today's wired world, the financial hurt that companies feel can grow even after the initial security breach. Once the bad news spreads online and through social media, it can hardly be undone.

Now Canadian companies face a new security and privacy challenge, but not from the latest technique deployed by hackers.

How can my business assess its security and privacy controls?

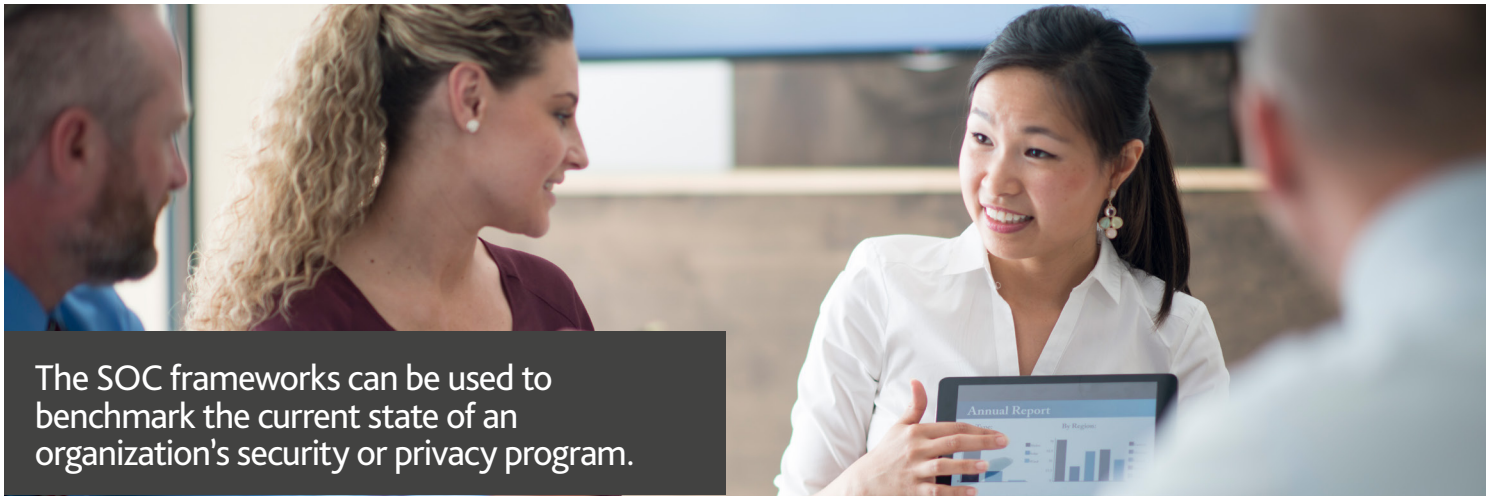
The self-assessment process can be kick-started by asking five key questions of your organization:

- Do you know where your data resides?
- Is your data secure and private?
- Is your data encryption robust and has it been independently tested?
- Have you assessed your personal liability and accountability risk?
- Have you developed a plan to conduct an independent readiness assessment and gap analysis?

System and organization controls (SOC) reports can serve as a key tool of your security self-assessment. SOC reports are designed to provide assurance on system and organization controls and processes related to various platforms.

The SOC frameworks can be used to benchmark the current state of an organization's security or privacy program. A SOC readiness assessment can help organizations identify deficient or insufficient controls, policies and procedures, and quantify security and privacy risks against a standard set of criteria. This gap analysis can be used to develop remediation strategies. An independent examination can be used to provide an unbiased, third-party assessment of the design and operating effectiveness of security and privacy controls.

BDO



The SOC frameworks can be used to benchmark the current state of an organization's security or privacy program.

More generally, SOC reports cover cloud-based environments, SaaS, infrastructure, software and financial systems, addressing factors such as security (including cybersecurity), privacy, confidentiality, availability and processing integrity. From data centres to fintech, SOC has become a necessary step of accountability for a wide variety of organizations. SOC reports are also in full compliance with Canada's CPA standard CSAE 3416 and the U.S. SSAE 18 standard, and they satisfy international ISAE standards.

What are the benefits of SOC reporting?

SOC reporting has come a long way since its earliest days. Its newest cybersecurity attestation standard, SOC for cybersecurity, is a critical addition to the SOC suite. Now, through a SOC engagement, your SOC audit partner can provide an independent assurance on your organization's system and organization controls (SOC 1, SOC 2, SOC 2+additional subject matter and SOC 3) or on entity-wide controls (SOC for cybersecurity).

Undertaking SOC attestation provides numerous benefits for an organization, including building trust with current customers and prospects. Most organizations partner with multiple external service providers and service organizations, and auditing each would be time consuming, inefficient and disruptive to both parties.

Other benefits include:

- **Strategic positioning.** For example, some companies are disqualified from bidding on new business without a proper SOC report. Obtaining one can increase participation and qualification in the RFP process.
- **Meeting obligations.** SOC helps you meet current and future contractual and service level agreement obligations and compliance.
- **Value proposition.** Your organization can enhance its organizational value by differentiating its value proposition.
- **Minding the gaps.** A SOC report can identify and close any gaps before they create actual operational deficiencies, reputational risk and loss of business. This allows organizations to address any potential breakdowns that could possibly lead to a breach.

In view of SOC's benefits to your organization, making a mistake is not an option. For certain highly regulated industries, compliance gaps can have legal consequences. SOC reports are sometimes not just a nice-to-have but a must-have.

Soc reporting guide: which SOC report is right for you?

SOC reporting	SOC 1	SOC 2 and SOC 2+ additional subject matter	SOC 3
SCOPE	Controls at a service organization relevant to user entities' (clients or prospects) internal controls over financial reporting.	**SOC 2** Controls over the security, availability, and processing integrity of a system, or the privacy or confidentiality of information processed by the system. **SOC 2+ additional subject matter** SOC 2+ reports include additional topics specific to users' unique requirements. Reporting on a service organization's compliance with a statement of privacy practices in addition to reporting on controls at the service organization relevant to the privacy of the system. If planned properly, this audit approach can reduce compliance costs and efforts by streamlining controls testing and combining assurance reporting in one report.	Same as SOC 2
REPORT COMPONENTS	A description of the service organization's system. Opinion on the fairness of the presentation of management's description of the system and the suitability of the design of the controls (Type 1). Type 2 reports also provide an opinion on the operating effectiveness of the controls, including detailed description of tests of controls performed by the service auditor, and results of those tests.	A description of the service organization's system. Opinion on the fairness of the presentation of management's description of the system and the suitability of the design of the controls (Type 1). Type 2 reports also provide an opinion on the operating effectiveness of the controls, including a detailed description of tests of controls performed by the service auditor, and results of those tests.	Opinion based on an unaudited description of the service organization's system on whether the entity maintained effective controls as it relates to the principle being reported on.
INTENDED USAGE	Service organization's management, user entities' management, user entities' financial auditors.	Same as SOC 1, plus knowledgeable parties—informed stakeholders, including appropriate business partners, prospective customers, vendor management executives and regulators.	General use
DISTRIBUTION	Restricted	Restricted	Unrestricted



Request a free consultation

How to select your SOC compliance partner

You want a SOC compliance partner that can work closely with you and tailor their approach to meet your unique needs and business requirements.

Contact us today for a preliminary assessment of your business requirements in determining which SOC report is right for you.

TO LEARN MORE, CONTACT YOUR LOCAL BDO OFFICE OR:

Sam Khoury, CPA, CITP, CRISC
Partner, Third Party Assurance
National Financial Services Leader
416-369-6030
skhoury@bdo.ca

ABOUT BDO

BDO is a leading provider of professional services to clients of all sizes in virtually all business sectors. Our team delivers a comprehensive range of assurance, accounting, tax, and advisory services, complemented by a deep industry knowledge gained from more than 100 years of working within local communities. As part of the international BDO network, we're able to provide seamless and consistent cross-border services to clients with global needs.

Assurance | Accounting | Tax | Advisory
www.bdo.ca

BDO Canada LLP, a Canadian limited liability partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.