Grant Thornton

An instinct for growth™

Managing virtual currency and blockchain risk with System and Organization Controls (SOC) attestation

The virtual asset space is developing at an astonishing rate. A technology that barely existed over a decade ago is now arguably spawning one of the greatest financial revolutions of our age—introducing countless innovative and never-before-seen products, services and business models. But just as it's hard to deny the tremendous potential this technology has to offer, it's difficult to ignore its associated risks—whether perceived or otherwise.

While the world made tremendous progress in 2018 from a virtual asset regulation and risk management perspective—incorporating the industry into existing and new regulatory and risk management frameworks—there is still a way to go. With no formally-enacted regulatory requirements or guidelines in place in Canada, virtual asset risk management is still a best practice undertaking—which means companies must take it upon themselves to ensure they're doing what it takes to protect the best interests of their customers.

To do this, they must look more critically—and thoroughly—at their internal control structures. One way of doing this is through undertaking a System and Organization Controls (SOC) attestation engagement.

Something we all have in common

As unique as the virtual asset industry is, there's one thing it shares in common with all others: consumers. As a result, success in this space is largely reliant on consumer trust. To earn it, virtual asset businesses need the ability to demonstrate good governance—and prove they're effectively managing their customer assets and information. Failure to do so can result in potentially damaging outcomes, for both customer and business.

Fortunately, the need for effective internal controls isn't new—and the virtual asset industry only needs to turn to more "traditional" financial and tech industries to see how to seek assurance in this arena. Assurance of this type is usually provided to companies through the issuance of a System and Organization Controls (SOC) report.

SOC reports have become an industry standard for providing assurance across a number of areas—most notably financial reporting and operations controls—and the virtual asset industry should be no different. Whether you're an exchange, custodian, wallet provider, fund or any other type of business responsible for storing and maintaining customer assets, these reports can go a long way to assure your customers, as well as key stakeholder groups such as banking partners, investors and the public, that you're acting responsibly with your customers' virtual assets.

An increasing number of players in the virtual asset industry are catching on to this reality—and this is encouraging. We believe these early adopters will have a significant leg up when SOC reports inevitably become a standard for this industry. If you're interested in joining their ranks, we've outlined a few things you need to know to get started.

A primer: What are SOC attestation engagements?

The purpose of a System and Organization Controls (SOC) engagement is to validate that a user entity (the recipient of services being provided by a third party) or service organization (the entity providing the services) is operating as efficiently as possible, while minimizing risks and offering the best quality service. These exams are performed by service auditors and must meet the attestation standards set out by the American Institute of Certified Public Accountants (AICPA) (for companies in the United States) and the Canadian Standard on Assurance Engagements (for companies situated in Canada).

The standards vary depending on the type of company and the subject matter being reported on. As such, they are broken down into three different types of reports: SOC 1, SOC 2 and SOC 3. There are different reasons why an entity might want to choose one over the other, which are outlined in the chart below:

[1]Question	SOC 1 report	SOC 2 report	SOC 3 report
What does the engagement test?	An organization's financial reporting controls.	An organization's controls relative to security, availability, processing integrity, confidentiality and/or privacy.	
What is the purpose of the engagement?	**To provide information to a relevant stakeholder (e.g., a user entity, including its auditors) about an organization's financial reporting controls**. It enables the user auditor to perform risk assessment procedures and, depending on the type of report sought, assess the risk of material misstatement of financial statement assertions.	**To provide an organization's management team,** as well as other specified parties, with a Certified/Chartered Professional Accountant's (CPA) opinion about controls at the organization that may affect the entity's security, availability, processing integrity, confidentiality or privacy.	**To provide interested parties (e.g., banking partners, investors, customers and the public)** with a Certified/Chartered Professional Accountant's (CPA) opinion about how an organization's existing controls may affect the entity's security, availability, processing integrity, confidentiality or privacy.
What is the outcome of the engagement?	**Type 1 report:** A report on the description of controls at a point in time, provided by management of the organization, which attests that the controls are suitably designed and implemented. **Type 2 report:** A report on the description of controls over a period of time, provided by management of the service organization, which attests that the controls are suitably designed and implemented, and attests to the operating effectiveness of the controls.		The auditor's report on whether the entity maintained effective controls over its system as it relates to the criteria being reported on (e.g., security, privacy, etc.)
Who is the audience/ intended user of the report?	**Restricted use** – SOC 1 reports are intended for auditors of the user entity's financial statements, management of the user entity and management of the service organization.	**Restricted use** – SOC 2 reports are intended for an audience that has prior knowledge and understanding of the system, such as management of an organization.	**Anyone** – SOC 3 reports can be shared openly with the public and posted on a company's website with a seal indicating their compliance.

1 www.aicpa.org/soc

SOC reporting considerations for virtual asset businesses

Given the unique nature of the virtual asset industry, it makes sense that a SOC engagement in this space would require new testing considerations. For instance, while the scope will inevitably include traditional factors—such as the organization's business model, the intended users of the report, and the objectives and timeframe sought by the business—it will also need to accommodate unique aspects about the type of virtual asset/blockchain business undertaking the engagement.

A virtual asset exchange or custodian, for example, would have a long list of specific crypto-related considerations, such as:

The management and governance of the wallet services system. Who has signature rights? What is the protocol in place around transaction execution? How well documented is this process?

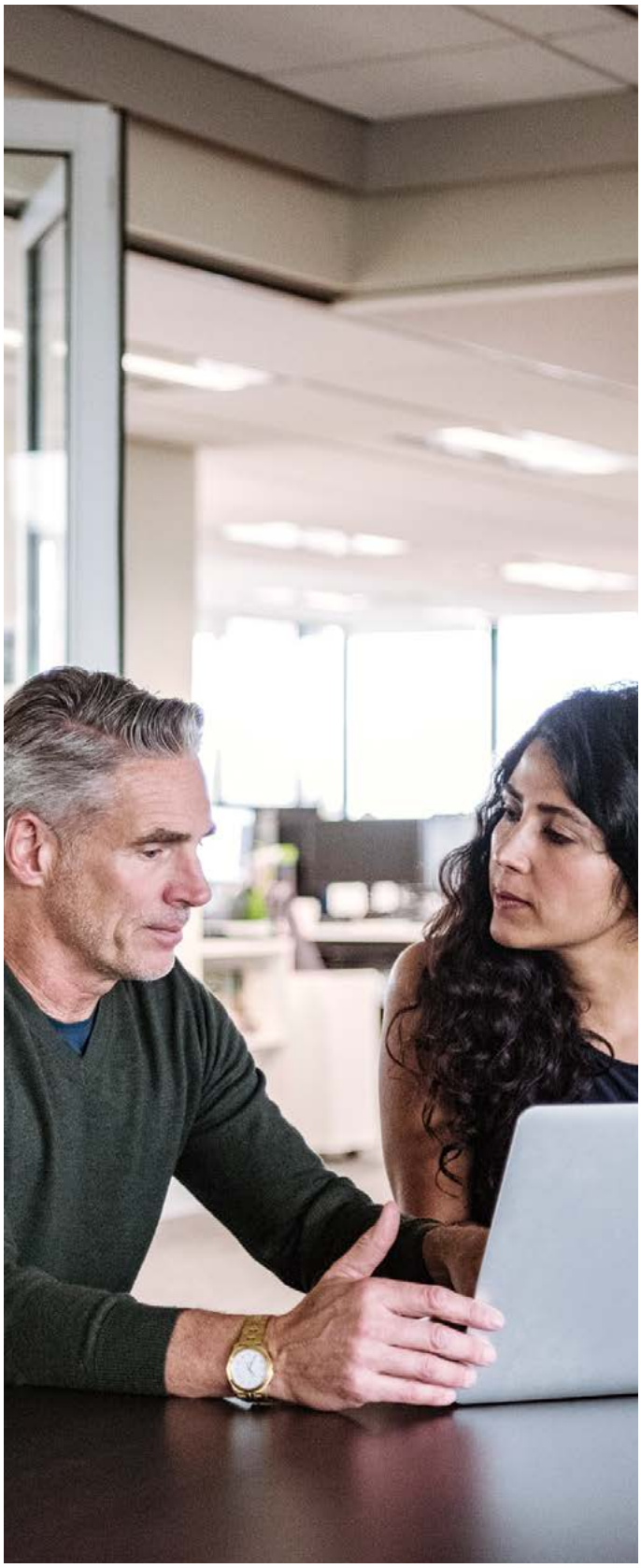
Cold storage of funds. Who has access to the cold storage? What encryption is placed around the keys? How are the private keys protected? What backups are in place in the event that the wallet is misplaced or stolen?

Physical security. What measures have been taken to ensure the security of the organization's premises? Who has personal custody of cold storage devices?

Coin/token management. In the case of an organization that operates its own coin or token, are there adequate, well-documented controls in place regarding the generation and destruction of that asset? How do the financial controls in the business align to this protocol?

Cybersecurity. What does the organization's cyber risk management framework look like? How effective are its cybersecurity controls?

Financial reporting. What is management's capacity to make decisions, direct the entity's activities and prepare financial statements? In a previous article, titled "Considerations for organizations in the virtual currency industry—the path to becoming audit ready," we explored the unique challenges presented to firms operating in the virtual currency space regarding preparation and audit of financial statements. This requires careful consideration and design, despite of still developing regulations in this area.



What's next?

It should be noted that the successful preparation and completion of a SOC engagement requires a significant investment of both time and resources. Companies will need to prepare policies, procedures and controls relating to a crypto and blockchain environment, in a manner that is consumable and subject to examination.

For many in this space, the focus has—up until now—been on maintaining and developing the commercial aspects of the business. As the industry matures, however, more attention will have to be paid to the design and documentation of policies and procedures. To do this, it might make sense to take a phased approach and address different aspects of an organization's systems over time.

To help in this endeavour, we've outlined four steps an organization can take toward the successful completion of a SOC report. These do not need to always be undertaken in sequence; the approach and stages required by an entity in this space will depend on the maturity of its organizational controls and the documentation around them.

1 Decide on the type of SOC report(s) required.

As described above, there are different types of SOC reports that can be undertaken depending on the end objective and requirements related to the need for assurance/attestation. The first stage would involve working with a professional to determine what type of attestation best suits your needs.

2 Conduct a readiness assessment for the desired SOC engagement.

This would first involve assessing which areas of your business are relevant to the SOC engagement—including key departments, points of contact and processes to be assessed. Following this, a readiness assessment of the agreed-upon areas should be conducted to determine how well your processes and controls are currently documented, and cataloguing gaps against expected standards and requirements of a SOC engagement.

3 Remediate gaps identified through the readiness assessment.

Following the readiness assessment, you would work with a professional to remediate any gaps in your process and control documentation—either by establishing new procedures, enhancing existing documentation, or both (depending on the outcomes of the readiness assessment).

4 Undertake the SOC engagement and produce a final report.

Upon completion of the readiness assessment and remediation of gaps against the assessment, the SOC engagement itself can be undertaken.

The power of advance preparation

Effective risk management is instrumental in building trust and ensuring the long-term success of the virtual asset/blockchain industry. By working with a professional with requisite knowledge of the SOC process—and ensuring your processes and controls are adequately prepared, documented and effective—you stand the best chance of protecting your organization and its customers from potentially irreparable damage in the future, and mitigating unforeseen delays and additional costs down the road. Grant Thornton provides risk advisory services to a range of businesses in the virtual asset industry. If you'd like to learn more about how our in-depth knowledge and industry-leading work preparing SOC reports can help protect your business and its customers—or if you'd simply like to learn more about how SOC engagements can enhance your business—contact us today.

Toronto

Jennifer Fiddian-Green, Partner
T +1 416 360 4957
E Jennifer.Fiddian-Green@ca.gt.com

David Florio, Partner
T +1 416 369 6415
E David.Florio@ca.gt.com

Giles Dixon, Manager
T +1 416 607 2689
E Giles.Dixon@ca.gt.com

Markham

Ali Jaffer, Senior Manager
T +1 416 607 2612
E Ali.Jaffer@ca.gt.com

Vancouver

Shane Troyer, Partner
T +1 604 443 2148
E Shane.Troyer@ca.gt.com

Mohammad Pahrbod, Senior Manager
T +1 604 443 2174
E Mohammad.Pahrbod@ca.gt.com

Grant Thornton
An instinct for growth™

grantthornton.ca

Audit | Tax | Advisory

About Grant Thornton in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member firms operate in over 130 countries worldwide.