More "As a Service" organizations are being started every day. In order to build trust with their customers and stakeholders, many organizations are exploring embarking on a SOC2 initiative for the first time. While there are many questions that organizations have about SOC2, there are 3 that stand out to me as "*guiding questions":*

1. What trust services criteria do I choose?
2. Do I need a Type 1, Type 2 or both?
3. What timeframe should my first Type 2 period cover?

Here is some guidance and answers to these questions based on my experience:

1. What trust services criteria do I choose for my first audit?

A SOC2 report can include some or all of the following trust services categories: Security, Availability, Confidentiality, Processing Integrity and Privacy. Organizations typically select Security as their baseline and add other categories if:

- Stakeholders request a SOC2 report covering specific trust categories
- Existing commitments (e.g. contracts) require certain criteria to be included
- The organization wishes to demonstrate unique properties of its system and controls in one or more of the other categories

The right answer is the one that satisfies the business and trust relationship between the organization and its stakeholders.

My recommendation: I regularly advise clients to limit their first SOC2 audit to Security and only include additional criteria if necessary. This will allow an organization to focus on the fundamental controls, being audited for the first time, and limiting disruption to the business. Additional categories can be added in subsequent periods as the business grows in size and sophistication.

2. Do I need a Type 1, Type 2 or both?

The following table describes some of the key similarities and differences between SOC2 Type 1 and Type 2 reports.

Topic	SOC2 Type 1	SOC2 Type 2
Contents of the report	1. Management Assertion 2. Auditor's Report 3. System Description 4. List of In-Scope Controls & Trust	1. Management Assertion 2. Auditor's Report 3. System Description 4. List of In-Scope Controls, Trust

	Principles	Principles, *Auditor's Tests & Results*
Scope of the audit and report	Focus on the *design* of controls	Focus on the *design* & *operating effectiveness* of controls
Time Frame covered by the audit and report	Point in time assessment (i.e. as of a specific date)	Period of time assessment (i.e. over an audit observation period of 3-12 months)
How quickly is the report available?	A typical audit and report can be completed within 4-6 weeks of *controls being implemented*	A typical audit and report is available 4-6 weeks *after the end of the audit observation period*
How long is the report valid?	The auditor's opinion is valid for up to 12 months. The Type 1 report is generally only performed once as an interim step to a Type 2. Many companies move to their first Type 2 within approximately 6 months.	The auditor's opinion is valid for up to 12 months at which point a new Type 2 audit and report must be completed.
What are some of the benefits?	• Ability to meet short-term stakeholder requirements for a SOC2 report • Independent confirmation up-front that the controls in place satisfy SOC2 requirements • Focus only on design makes it easier for some organizations new to audit & compliance to achieve	• Report is generally considered more useful by stakeholders as it covers *design* & *operating effectiveness* • Demonstrates a commitment to an organization's ability to maintain and operate a well controlled system *over a period of time* • May be less expensive by going directly to Type 2
What are some of the drawbacks?	• Generally viewed by stakeholders as an *interim* way of satisfying their requirements • Could lead to a false sense of comfort that the controls will work as expected when called upon • Incremental cost of performing two audits in the first year (Type 1 and Type 2)	• Longer period of time before SOC2 report and auditor's opinion are available to stakeholders • Higher risk that the first audit will have exceptions or qualifications due to controls not operating as expected or intended.

My recommendation: I generally recommend first timers start with a Type 1 followed by a Type 2 six months later. This allows you to get an independent perspective on the design of your controls (and the

ability to share this with your stakeholders) while establishing the cadence of operating them on an ongoing basis. This also generally makes the Type 2 audit process more straightforward as most issues should have already been worked through.

3. What timeframe should my first Type 2 cover?

A typical SOC2 Type 2 report covers a 12 month period (does not have to align to a calendar year). However, many organizations want their first SOC2 Type 2 report to be completed earlier, especially if they did not complete a Type 1 report. Many auditors will accommodate an audit observation period between *3 and 12 months.*

My recommendation: I suggest 6 months as the "sweet spot" for the first Type 2 audit and report. Why?:

- This provides for sufficient time to demonstrate the operating effectiveness of all controls (some periodic or annual controls may not naturally fit within a 3 month audit period)
- Provides for a greater opportunity to mitigate the impact of exceptions (the more samples available for testing the lesser the impact of individual exceptions)
- Enables stakeholders to get the first report in a relatively timely manner
- If the auditor's report is qualified, allows for another audit to be performed within the original 12 month window.

Most auditors will also provide a letter confirming your engagement and the estimated completion of the audit and SOC2 Type 2 report.

MHM Professional Corporation, Chartered Professional Accountant

MHM Professional Corporation is an independent CPA firm led by Mark Mandel, an ex-Big 4 Partner with over 20 years of Assurance & Consulting experience. Mark brings deep expertise in Audit, Digital Trust, & Data Analytics and has a wealth of experience with IT controls & security standards supporting SOC1, SOC2, PCI, SOX and financial audits.

MHM brings a practical approach to delivering on IT audits. By focusing on the key principles of scoping & risk mitigation and leveraging technology to its fullest, MHM is able to provide small & medium sized private companies with an **affordable, efficient approach to SOC2 audit and compliance** by bringing Big 4 expertise without the expense.