WHY MULTIPLE ANSWERS MAY BE THE RIGHT ONE

schellman

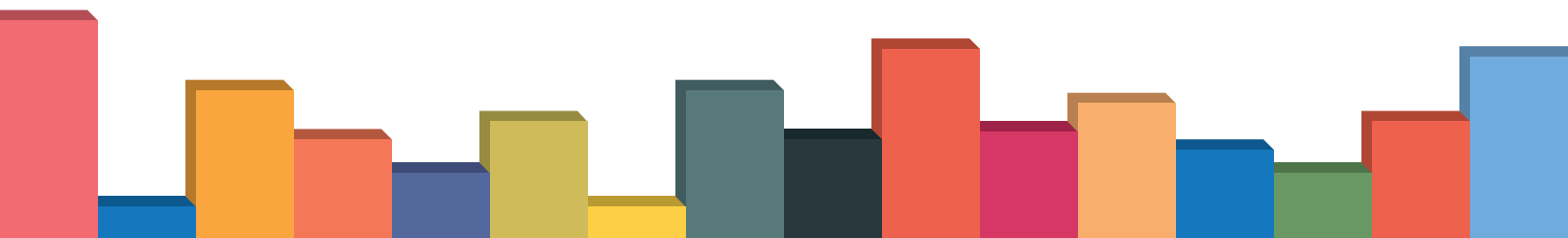
Quality, above all.

WHY MULTIPLE ANSWERS MAY BE THE RIGHT ONE

Organizations in the market for third party assurance on their information security controls and programs often wonder which audit is best for them, and, more importantly, which one is best for their requesting customers. They ask questions like, "would the ISO 27001 certification meet a customer's needs better than a SOC 1 or SOC 2 examination report? These conversations are common, and the answer is that there are options.

The most important factor when considering these examination and certification options is remembering that they all have a different objective and serve a different purpose. For the most common examinations or certifications that we encounter, we have created a table that includes a brief overview of these examinations and certifications, in addition to their focus, term, deliverable, audience and uniqueness. After some thought, what most organizations end up realizing is, that in today's market, achieving multiple examinations and certifications is the best approach.

Here is why...



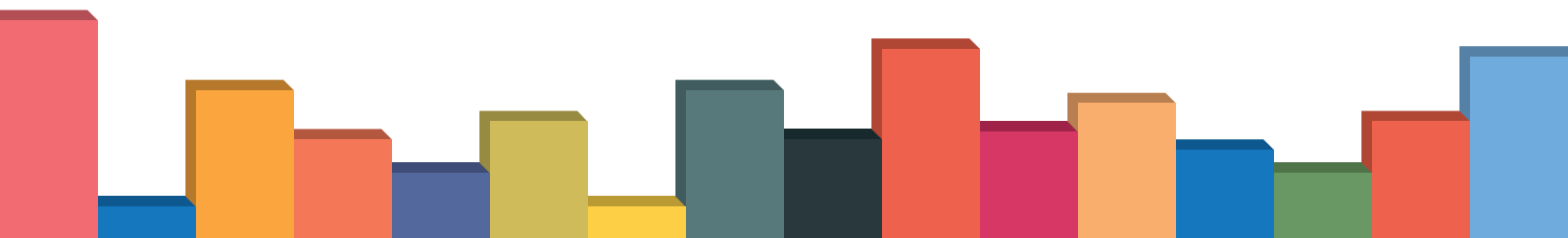
SOC 1 EXAMINATIONS

SOC 1 examinations can be a contractual requirement for organizations that provide a service to their customers if that service provided has a financial reporting impact. The report includes control objectives and control activities that are tailored to the service organization and then presented in a SOC 1 report--either a Type 1 or Type 2—and these are relied upon by the customer's financial auditors.

> Aside from possibly being a requirement, the SOC 1 report is also beneficial in that it is a report that is specific to the organization and pertinent to its customers.

The system description includes a narrative regarding the organizational control environment, as well as process narratives detailing the services within the scope of the review.

However, the SOC 1, is limited in its use in that its intention is only for customer financial auditor reliance. Prospects and other customers that may not rely on the organization's services for their financial reporting purposes have no use for the SOC 1 report. And though the uniqueness of the report can be a positive, it can also be seen as undesirable, as the controls and objectives are determined by the organization, which prevents any common criteria comparison from report to report.

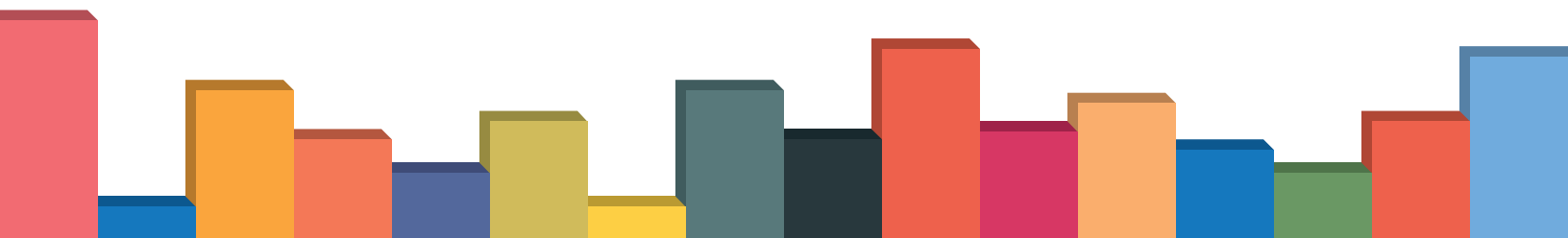


SOC 2 EXAMINATIONS

SOC 2 examinations are gaining popularity as more organizations understand their value and purpose. Like the SOC 1, the SOC 2 examination can be performed as a Type 1 or a Type 2. With the SOC 2, the organization is responsible for determining which Trust Services Principles are included within the scope of the review, and they are also responsible for defining the controls activities that are in place to meet the criteria of those in-scope principles. The system description of a SOC 2 includes a narrative on the organization's applicable infrastructure, applications, people, processes and data that are within the scope of the examination, as well as a narrative regarding the organizational control environment.

The SOC 2 report is intended for any audience, including current customers and prospects. In addition, as the criteria within the principles are pre-defined, the SOC 2 report allows for comparison with other SOC 2 reports while letting readers of the report gauge how an organization measures up to the criteria within the selected principles. Additionally, the criteria touch the key elements of information security within the applicable principle.

That being said, the SOC 2 is not a silver bullet. Like the SOC 1, it is a controls-focused audit and includes either a point-in-time assessment, in the case of a Type 1, or a backward-looking evaluation, in the case of a Type 2. Though an expansive presentation, the report is already historic once issued, which is by design.

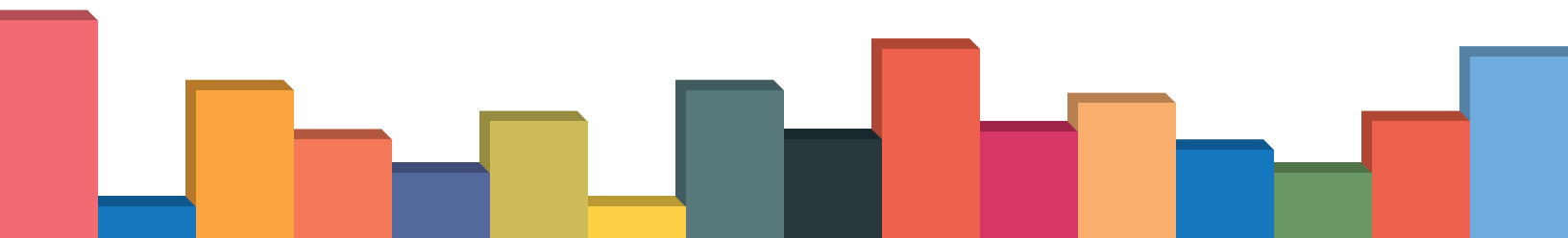


CSA STAR ATTESTATION

CSA STAR Attestation is a collaboration between the CSA and the American Institute of CPAs (AICPA) to provide guidance for STAR Attestations using criteria from the AICPA Trust Services Principles and the Cloud Control Matrix (CCM). This assessment utilizes the SOC 2 framework to report on a cloud service provider's controls relevant to the applicable Trust Services Principles and the criteria in the CSA CCM. It can be performed in a Type 1 format to determine the suitability of the design of the controls in place, or in a Type 2 format to determine the suitability of the design and operating effectiveness of its controls. The report mirrors the same components of a SOC 2 report with the addition of the CCM control testing.

Much like the SOC 2, the CSA STAR Attestation report can be provided to customers or prospects as a means of communicating the details of the cloud service provider's system, the controls in place and the results of the testing applied to those controls. Also similar to the SOC 2 examination, customers of a cloud service provider can evaluate one CSA STAR Attestation report against another and have a legitimate comparison between the two, as both were assessed against the same criteria.

Again alike to the SOC 2 examination, the CSA STAR Attestation report is a regressive-looking document that provides the operational results of controls that already occurred. The report is meant to be relied upon, but is not actively relevant after the review period has ended. Also, the CSA STAR Attestation is only applicable for cloud service providers.



ISO 27001 CERTIFICATION

Like the SOC 2, ISO 27001 certification is also gaining popularity—though for different reasons. ISO 27001 standard outlines the requirements for constructing a risk-based framework to initiate, implement, maintain, and manage information security within an organization. The standard defines what an information security management system (ISMS) is, what is required to be included within the ISMS, and how management should form, monitor, and maintain the ISMS. The fundamental components of an ISMS include the 1) risk assessment based on the risk to confidentiality, integrity, and availability of data within scope of the ISMS, 2) treatment of risk to include the consideration of the 114 controls within 14 different domains from Annex A of the standard, 3) continuous monitoring of the selected controls to ensure that they are operating effectively, 4) internal audit on the controls and ISMS requirements to ensure that they maintain conformance, and 5) management review of the holistic ISMS to identify areas of improvement and continuous growth.

To achieve ISO 27001 certification, the organization has to evidence full conformance to the requirements within the standard. Once certified, the certificate is valid for a term of three years, assuming that annual surveillance reviews are maintained to confirm continued conformance to the standard. It is intended to be an active ISMS, meaning that it is continuously operating effectively (as opposed to the point-in-time or backward-looking control assessment of the SOC 1 and SOC 2 noted above). In basic terms, customers and prospects can gain assurance that the certified scope has management support, communicates the value of information security within that scope, and has the right people performing the right tasks for the right controls at the right time.

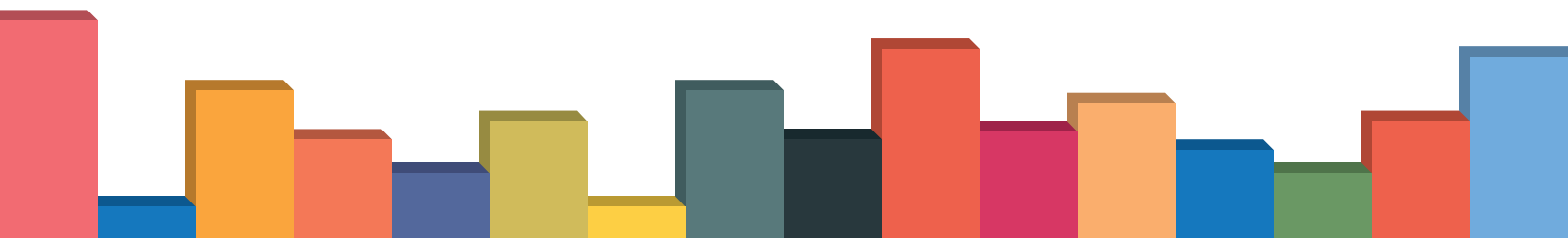
Unlike the SOC 1 or SOC 2, the external deliverable for ISO 27001 is only a certificate and does not include a full external report. A full description of the fundamental elements of the scope is not disclosed, nor are the controls or any exceptions for that matter. The certificate requires a level of trust from the recipient, as it does not assure any details.

CSA STAR CERTIFICATION

The CSA STAR Certification is directly related to the ISO 27001 certification. As a matter of fact, you cannot achieve CSA STAR certification if you do not have an active ISO 27001 certification (though you can achieve both concurrently). The CSA STAR Certification leverages the ISMS from a management system perspective, but focuses on an organization's maturity level with regard to the controls in the CCM. A maturity score is given for each control, and the lowest control score is applied to the domain score, which is then averaged across all CCM domains to result in the overall maturity score. This overall maturity score is communicated to the organization but not included on the external certificate.

> For cloud service providers that are already ISO 27001 certified, the CSA STAR Certification is a compliment to the ISMS.

It is another means for the organization to communicate that they have been measured against the CCM, and because of their leadership, communication, training, processes, controls and monitoring, they have achieved a maturity level that warrants a certificate. But like the ISO 27001 certificate, the resulting deliverable is only the certificate—there is no substantive, detailed report to support the details that merit the award.



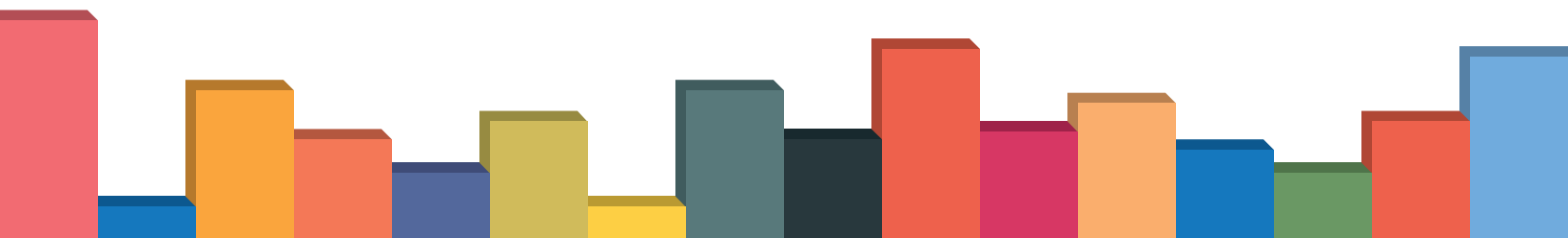
GETTING STARTED

- Review your corporate strategy and/or compliance roadmap
- Obtain a listing of your current compliance inventory
- Review the results of your past audits
- Discuss with your stakeholders audit goals

CONTACT US TODAY

Schellman offers several competitive differentiators for Organizations looking to make the most out of their compliance initiatives. We are the first CPA firm that is 100% independent with no consulting agenda. And are a trusted provider to the world's leading companies and the only company in the world capable of providing SOC, PCI, ISO, FedRAMP, and HITRUST services through a single legal entity. We also offer organizations the opportunity to consult with our distinguished subject matter experts.

For more information or to contact us about your compliance initiatives, go to schellman.com




schellman