MOST COMMON EXAMINATIONS: COMPARED

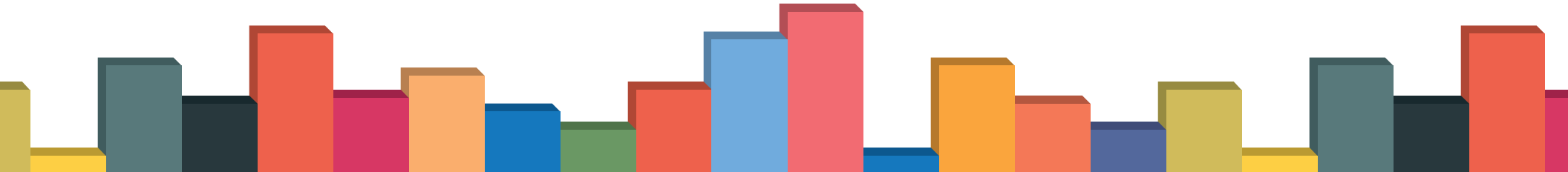
schellman

CRUCIAL PROCESSES

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.

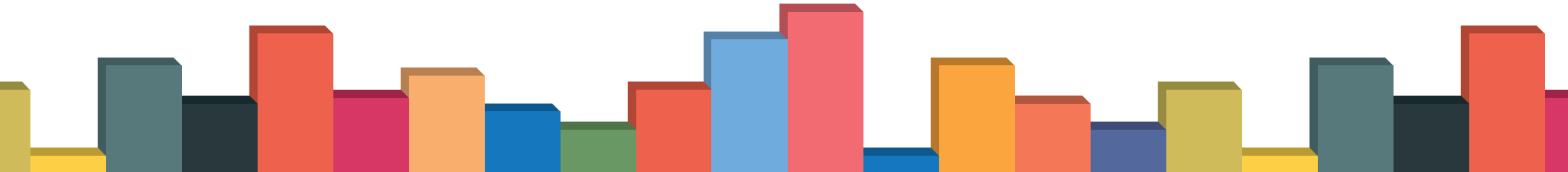
The most important factor when considering these examination and certification options is remembering that they all have a different objective and serve a different purpose. For the most common examinations or certifications that we encounter, we have created this table to include a brief overview of these examinations and certifications, in addition to their focus, term, deliverable, audience and uniqueness. For further explination on why so many companies we work with end up choosing multiple examinations, get our piece on why choosing multiple services may be the right choice.

TYPE	FOCUS	TERM	DELIVERABLE	AUDIENCE	UNIQUENESS
SOC 1 Type 1	Control activities supporting control objectives defined by the organization that are relevant to services provide to customers that have a financial reporting impact.	The control activities are assessed as of a review date.	SOC 1 Type 1 report which includes an opinion from the CPA firm on the fair presentation and design of the control set supporting the control objectives.	Customers that rely on the organization for services that have a financial reporting impact.	The control set within a SOC 1 report is unique to the organization. The report can be combined with the ISAE 3402 requirements to produce an internationally accepted report.
SOC 1 Type 2	Control activities supporting control objectives defined by the organization that are relevant to services provide to customers that have a financial reporting impact.	The control activities are tested against a review period, typically a minimum of six months and defined by the organization.	SOC 1 Type 2 report which includes an opinion from the CPA firm on the fair presentation, design, and operating effectiveness during the review period of the control set supporting the control objectives.		
SOC 2 Type 1	Control activities meeting the applicable criteria of the in-scope Trust Services Principles, which are determined by the organization and include Security, Availability, Confidentiality, Processing Integrity, and Privacy.	The control activities are assessed as of a review date.	SOC 2 Type 1 report which includes an opinion from the CPA firm on the fair presentation and design of the control set supporting the applicable criteria within the selected Trust Services Principles.	Customers or prospects. The SOC 2 report is intended for any audience that would have an interest in the controls of the organization.	The criteria in the SOC 2 Trust Services Principles include a prescriptive control set which allows recipients of the report to gauge the organizations controls that are in place, and operating effectively in the case of a Type 2, to meet the applicable criteria.



CRUCIAL PROCESSES

TYPE	FOCUS	TERM	DELIVERABLE	AUDIENCE	UNIQUENESS
SOC 2 Type 2	Control activities meeting the applicable criteria of the in-scope Trust Services Principles, which are determined by the organization and include Security, Availability, Confidentiality, Processing Integrity, and Privacy.	The control activities are tested against a review period, typically a minimum of six months and defined by the organization.	SOC 2 Type 2 report which includes an opinion from the CPA firm on the fair presentation, design, and operating effectiveness during the review period of the control set supporting the applicable criteria within the selected Trust Services Principles.		
CSA STAR Attestation Type 1	Control activities meeting the applicable controls in the cloud control matrix (CCM) in addition to the applicable criteria of the in-scope Trust Services Principles, which are determined by the organization and include Security, Availability, Confidentiality, Processing Integrity, and Privacy.	The control activities are assessed as of a review date.	CSA STAR Attestation SOC 2 Type 1 report which includes an opinion from the CPA firm on the fair presentation and design of the control set supporting the applicable controls within the CCM as well as the applicable criteria within the selected Trust Services Principles.	Customers or prospects. The CSA STAR Attestation SOC 2 report is intended for any audience that would have an interest in the controls of the organization.	In addition to the uniqueness noted for the SOC 2 examination, this option is applicable to only cloud service providers. A Type 1 examination can be performed only once; thereafter, the cloud service provider is required to move to a Type 2 report. Upon completion of the CSA STAR Attestation, the cloud service provider can register on the CSA STAR Registry.
CSA STAR Attestation Type 2	Control activities meeting the applicable controls in the CCM in addition to the applicable criteria of the in-scope Trust Services Principles, which are determined by the organization and include Security, Availability, Confidentiality, Processing Integrity, and Privacy.	The control activities are tested against a review period, typically a minimum of six months and defined by the organization.	CSA STAR Attestation SOC 2 Type 2 report which includes an opinion from the CPA firm on the fair presentation, design, and operating effectiveness during the review period of the control set supporting the applicable controls within the CCM as well as the applicable criteria within the selected Trust Services Principles.		

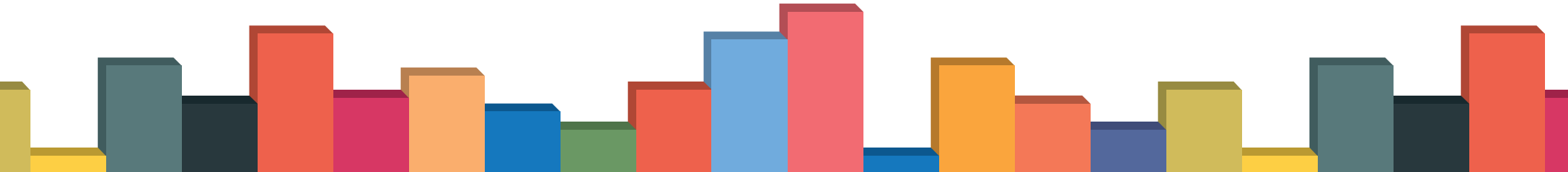


CRUCIAL PROCESSES

TYPE	FOCUS	TERM	DELIVERABLE	AUDIENCE	UNIQUENESS
ISO 27001	The design, implementation, and operating effectiveness of the information security management system (ISMS) and supporting controls in Annex A in conformance of the requirements of ISO 27001:2013.	The certificate, once issued, is valid for a three year term, which requires annual surveillance audits to ensure continued conformance with the requirements of ISO 27001:2013.	An ISO 27001:2013 certificate which includes the scope statement of the certified ISMS as well as the locations included within the scope of the review and the dates of issuance and expiration.	Customers or prospects. The certificate is a formal way to communicate that the organization maintains an ISMS in conformance of the ISO 27001:2013 standard.	As the ISO certification is not a controls focused audit, there is substantial effort on the organization's part to implement the ISMS. However, the achievement of the certificate demonstrates that the organization has an active management system.
CSA STAR Certification	The maturity level of an organization applicable to the controls in the CCM in addition to the conformance of the ISMS to the ISO 27001 requirements.	The certificate, once issued, is valid for a three year term, which requires annual surveillance audits to ensure continued conformance with the requirements of ISO 27001:2013 as well the maturity of the organization applicable to the controls in the CCM.	A CSA STAR certificate which includes the scope statement of the CSA STAR program as well as the locations included within the scope of the review and the dates of issuance and expiration.	Customers or prospects. The certificate is a formal way to communicate that the organization maintains an ISMS in conformance of the ISO 27001:2013 standard as well as has achieved a maturity level of the CSA STAR Certificate program to warrant the award.	An active ISO 27001:2013 certificate is a prerequisite to achieve the CSA STAR Certification. However, the ISO 27001 and CSA STAR certification audits can be performed in tandem. Upon completion of the CSA STAR Certification, the cloud service provider can register on the CSA STAR Registry.

GETTING STARTED

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




schellman