SOC1 vs. SOC2 vs. SOC3

Source:

http://www.ssae16.org/white-papers/soc-1-vs-soc-2.html

http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC3Report.aspx

SOC Reports

* Officially, SOC standards for "Service Organization Control", which allows qualified practitioners (i.e., licensed and registered Certified Public Accountants) to issue SOC 1, SOC 2, and/or SOC 3 reports. With the SSAE 16 standard (which is used for issuing SOC 1 reports) effectively replacing the longstanding SAS 70 auditing standard for reporting periods ending on or after June 15, 2011

SOC1

* Service Organization Control (SOC) 1 reports are to be conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, the AICPA "attest" standard that, not only replaced SAS 70, but was intended to reinforce SAS 70's true intent, which was an audit conducted over "internal controls over financial reporting", more commonly known as the ICFR concept.
* Because SAS 70 strayed heavily from its intended use, the newly formed SOC framework placed great emphasis on the ICFR component for service organization reporting, thus advocating service organizations to opt for a SOC 1 (for which you can obtain an SSAE 16 Type 1 or Type 2 report) only if your organization has a true relationship and/or nexus with ICFR.

SOC2

* To meet the growing needs of the ever-expanding technology companies who are classified as service organization for SOC reporting, the AICPA put forth the SOC 2 framework, a reporting option specifically designed for entities such as data centers, I.T. managed services, software as a service (SaaS) vendors, and many other technology and cloud-computing based businesses.

SOC2

* And within the SOC 2 framework is a comprehensive set of criteria known as the Trust Services Principles (TSP) that are composed of the following five (5) sections:
  * The security of a service organization' system.
  * The availability of a service organization's system.
  * The processing integrity of a service organization's system.
  * The confidentiality of the information that the service organization's system processes or maintains for user entities.
  * The privacy of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities.

SOC1 vs. SOC2

* **Intended Subject Matter and Applicable Scope:**
    - SOC 1: Internal Controls over Financial Reporting (ICFR).
    - SOC 2: Controls at a service organization that are relevant to security, availability, processing integrity confidentiality, or privacy.

* **Intended Users of each Report:**
    - SOC 1: External financial statements auditor's of the user organization's financial statements, management of the user organizations, and management of the service organization.
    - SOC 2: Relevant parties that are knowledgeable about the services provided by the actual service organization and that they have a true and credible need for utilizing a SOC 2 report.

SOC3

* SOC 3^{sm} reports are designed to meet the needs of uses who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2^{sm} report. These reports are prepared using the AICPA/ CPA Canada (formerly Canadian Institute of Chartered Accountants) Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because SOC 3^{sm} reports are general use reports, they can be freely distributed or posted on a website as a seal.

SOC2 vs. SOC3

* Trust Services Report for Service Organization: SOC 3 engagements use the predefined criteria in Trust Services Principles, Criteria and Illustrations that also are used in SOC 2 engagements.
* The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor's tests of controls and results of those tests as well as the service auditor's opinion on the description of the service organization's system. A SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria. **There is no description of tests and results or opinion on the description of the system.** It also permits the service organization to use the SOC 3 seal on its website. SOC 3 reports can be issued on one or multiple Trust Services principles, which are security, availability, processing integrity, confidentiality and privacy.