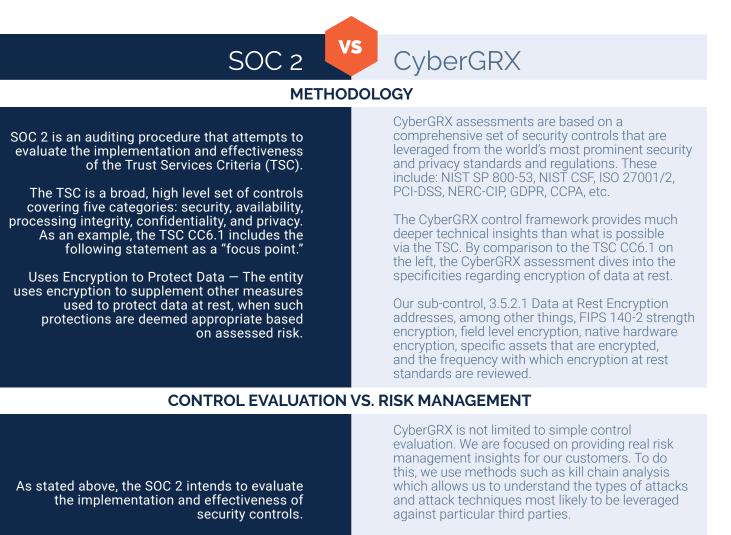


# SOC 2 & CyberGRX: What's the Difference?

A Service Organizational Control 2 (SOC 2) audit and a CyberGRX assessment may appear to be quite similar at first glance, but there are very distinct and important differences between these two security products. The following table describes these disparities.



This analysis highlights specific controls in our assessment that are most critical to the security posture of the third party. CyberGRX utilizes the MITRE ATT&CK matrix to develop kill chains.

#### ASSESSMENT TIME FRAME

Third parties can and are encouraged to update their CyberGRX assessments as changes occur in their security programs.

In addition, we update our threat intelligence feeds daily, which can illustrate changes in the threat landscape and resulting risk gaps associated with specific third parties.

A SOC 2 Type 1 is a point-in-time assessment.





### ASSESSMENT SCOPE

The scope of a SOC 2 is determined by the assessed organization and their auditor. This scoping includes the products and services that will be assessed, as well as the controls from the TSC that will be included. Oftentimes an SOC 2 will exclude entire categories of controls. In addition, there is no specificity to the controls in a SOC 2 beyond the previous example. This means that the results of any two SOC reports may be wildly different. CyberGRX offers three tiers of assessment that can be used to customize the level of rigor applied to the third party. Beyond that, there is no mechanism by which the third party can "scope out" controls or questions.

This means that our customers benefit from a standardized assessment process and output. In addition, this allows for an "apples to apples" comparison between third parties assessed via CyberGRX.

## **DATA VALIDATION**

SOC 2 audits and certification are provided by auditors from Certified Public Accounting (CPA) firms. The certification is based on the opinion of the auditor, so SOC 2 reports can vary significantly based on the capability, experience, and professionalism of the auditor.

SOC 2 audits are typically time consuming and

barrier for organizations, particularly small and

expensive to complete. This can be a major

medium-sized businesses.

CyberGRX applies the same proprietary risk analysis algorithms against all assessments.

These algorithms utilize the kill chain analysis previously described, combined with security scan results, threat intelligence feeds, inherent risk data, and a third party's assessment answers to provide standardized, data driven output.

#### PRICING

Third parties do not pay anything to complete a CyberGRX assessment.

The CyberGRX Exchange model means that there are thousands of up-to-date third-party assessments available at any moment. All our customers need to do is identify the third parties they use and request access to their assessments. If the third parties already have a completed assessment on the Exchange, the entire process from request to authorization can take a matter of minutes.

If the third party has not yet completed a CyberGRX assessment, the "crowd-sourced" demand created by the Exchange can be the catalyst to propel them into action. Our user-friendly web interface and dedicated support teams result in most assessments being delivered within a matter of weeks.

If you're looking for an innovative, dynamic approach to TPCRM, **schedule a demo** or read our **Vendor Risk Management Guide** to learn more.



© Copyright CyberGRX 2020