Compliance offerings by category

Certifications / attestations / reports

An independent third-party auditor has granted a formal certification, attestation, or audit report based on the assessment that affirms our compliance with these offerings.

ISO/IEC 27001 | PCI DSS | SOC 2 | SOC 3

GLOBAL | ALL INDUSTRIES

ISO/IEC 27001

The International Organization for Standardization (ISO) is an independent, non-governmental international organization with an international membership of 163 national standards bodies. The ISO/IEC 27000 family of standards helps organizations keep their information assets secure.

ISO/IEC 27001 outlines and provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks.

Chronicle Security product and the Uppercase service are certified as ISO/IEC 27001 compliant. The 27001 standard does not mandate specific information security controls, but the framework and checklist of controls it lays out allow Google to ensure a comprehensive and continually improving model for security management.

Related documents:
Chronicle ISO/IEC 27001 Certificate

GLOBAL | ALL INDUSTRIES

PCI DSS

The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. The Standards Council was established by the major credit card associations (Visa, MasterCard, American Express, Discover, JCB) as a separate organization to define appropriate practices that merchants and service providers should follow to protect cardholder data. It is this council of companies that created the Payment Card Industry (PCI) Data Security Standards (DSS).

PCI DSS is a set of network security and business best practices guidelines adopted by the PCI Security Standards Council to establish a "minimum security standard" to protect customers' payment card information. The scope of the PCI DSS includes all systems, networks, and applications that process, store, or transmit cardholder data, and also systems that are used to secure and log access to the systems in scope.

Chronicle Security product and the Uppercase service have been reviewed by an independent Qualified Security Assessor and determined to be PCI DSS 3.2.1 compliant. This means that these services provide an infrastructure upon which customers may build their own service or application which stores, processes, or transmits cardholder data. We have created this matrix to help explain the shared responsibility between Google and its customers.

Chronicle's PCI-DSS certification doesn't include the Looker feature.

Related documents:
Chronicle: PCI Shared Responsibility Matrix

GLOBAL | ALL INDUSTRIES

SOC 2

The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC). The purpose of this report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy.

SSAE 18 / ISAE 3402 Type II
The AICPA created the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) to keep pace with globally recognized international accounting standards. SSAE 18 aligns closely with the International Standard on Assurance Engagements 3402 (ISAE 3402), both of which are used to generate a report by an objective third party attesting to a set of assertions made by an organization about its controls. The Service Organization Controls (SOC) framework is the method by which the control of financial information is measured.

Chronicle undergoes a regular third-party audit to certify individual products against this standard.

Potential customers can reach out to sales for get a copy of our report.

Related Documents:
AICPA
SOC 2

GLOBAL | ALL INDUSTRIES

SOC 3

Like SOC 2, the SOC 3 report has been developed based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) Trust Service Criteria (TSC). The SOC 3 is a public report of internal controls over security, availability, processing integrity, and confidentiality.

SSAE 18 / ISAE 3402 Type II
The AICPA created the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) to keep pace with globally recognized international accounting standards. SSAE 18 aligns closely with the International Standard on Assurance Engagements 3402 (ISAE 3402).

SSAE 18 and ISAE 3402 are used to generate a report by an objective third-party attesting to a set of assertions made by an organization about its controls. The Service Organization Controls (SOC) framework is the method by which the control of financial information is measured.

Chronicle undergoes a regular third-party audit to certify individual products against this standard.

Potential customers can reach out to sales for get a copy of our report.

Related Documents:
AICPA
SOC 3