

## Google Security Audits and Certifications

At Google, ensuring the security of our users is a top priority, and we are constantly assessing how we can make our services even more secure. Google regularly undergoes independent verification of security, privacy and compliance controls. This means an independent auditor examines the controls present in our data centers, infrastructure and operations. These audits and certifications by accredited third-party auditors help verify the data protection technologies and processes Google is using, and show our commitment to protecting user data.



### International Standards Organization (ISO) 27001 Certification

ISO 27001 is a widely recognized, internationally accepted independent security standard. Google's ISO 27001 certification covers the systems, applications, people, technology, processes, and data centers supporting Google Apps for Business and Google Apps for Education. Our compliance with the ISO 27001 standard was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council, a member of the International Accreditation Forum (IAF). Certificates issued by Ernst & Young CertifyPoint are recognized as valid certificates in all countries with an IAF membership<sup>1</sup>.



The ISO 27001 certification is composed of 114 controls. Highlights of Google's certification include certifying:

- Information security policies
- Organization of information security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Logical security
- Incident management

Auditors: Ernst & Young CertifyPoint

<sup>1</sup> IAF Member Countries - [http://www.iaf.nu/articles/IAF\\_MEMBERS\\_SIGNATORIES/4](http://www.iaf.nu/articles/IAF_MEMBERS_SIGNATORIES/4)



Auditors: Ernst & Young LLP

## SSAE 16/ISAE 3402 and SOC 2 Type II Audit

A Service Organization Control (SOC) 2 report has a predefined set of principles and related criteria that are defined by American Institute of Certified Public Accountants (AICPA) and must be met to achieve an unqualified report. The criteria and report are widely recognized, and easily aligned with or compared to ISO 27001, National Institute for Standards & Technology (NIST) 800-53 and/or Control Objectives for Information and Related Technology (COBIT) information security frameworks.

The Principles covered in the report include:

- Security: The system is protected against unauthorized access (physical and logical).
- Confidentiality: The system has controls so data that is stored in the cloud is shared with only the people you wish to share it with.
- Processing Integrity: The system performs as you expect it to. Data is preserved to be the way you left it the last time you logged on.
- Availability: The system has mechanisms to prevent or quickly correct any service outages, including redundant sites that are in place for business continuity and backup and recovery of customer data. Ernst & Young LLP completed its procedures for the SOC 2 Type II audit and noted no deviations from the specified criteria during the period of the report.

Major control objectives and control activities covered by the audit include the following:

- Logical security controls provide reasonable assurance that logical access to production systems is restricted to authorized individuals.
- Data center physical security controls provide reasonable assurance that Google data centers and corporate offices are protected.
- Incident management controls provide reasonable assurance that system
- Change management controls provide reasonable assurance that application and configuration changes are tracked, approved, tested and validated.
- Organization and administration controls provide reasonable assurance that management provides the infrastructure and mechanisms to track and communicate initiatives, monitor compliance within the company and provide security training for the risks that impact Google.
- System availability controls provide reasonable assurance that redundant sites are in place for services and recovery of customer data is possible.

**Overall conclusion:** Ernst & Young issued an unqualified opinion with zero exceptions on any control objectives or control activities during the period for of the report.

**Time period covered:** May 1, 2013 to April 30, 2014<sup>2</sup>

**Report types:** Service Organization Control (SOC) 2 Type II reports are attestation reports issued by independent auditors under standards provided by the Auditing Standards Board (ASB) of the AICPA. Google's SOC 2 report covers the Security, Confidentiality, Processing Integrity, and Availability principles set forth in the AICPA's Trust Services Principles and Criteria.



**Updated:** August 2014

<sup>2</sup> Due to the nature of SSAE 16 / ISAE 3402 SOC 2 these audits will always reflect a time-frame that has passed. Audit reports only measure controls at a point in time. The audit date may be in the past, but it is our current audit and has not expired.

**Google Apps for Business and Google Apps for Education security audits and certification summary.**

Products and Services Covered		
Google Drive	●	●
Google Hangouts	●	●
Gmail	●	●
Google Calendar	●	●
Google Docs	●	●
Google Sheets	●	●
Google Slides	●	●
Google Apps Vault	●	●
Google Sites	●	●
Google Admin console <sup>3</sup>	●	●
Google Contacts	●	●
Google Apps Script	●	●
Google+	●	●
Google Now	●	●
Google Groups	●	●
Google Talk	●	●
Directory API <sup>4</sup>	●	●
Reports API <sup>5</sup>	●	●
SAML Based SSO API	●	●

**Google Cloud Platform security audits and certification summary.**

Products and Services Covered		
Google Apps Engine	●	●
Google Cloud Storage	●	●
Google Compute Engine	●	●
Google Cloud Datastore	●	●
Google Big Query	●	●
Google Cloud SQL	●	●

<sup>3</sup> Formerly Control Panel

<sup>4</sup> Formerly Directory Sync, and Provisioning API

<sup>5</sup> Formerly reporting API, and Audit API, and Audit API

