Google Apps for Business Audit & Certification Summary

ISO 27001 Certification

Auditors: Ernst & Young Certify Point

Services Covered: GMail, Google Talk, Google Calendar, Google Docs (documents, spreadsheets, presentations), Google Sites, Control Panel (CPanel), Google Contacts, Google Video, Google Groups, Directory Sync, Provisioning API, SAML-Based SSO API, Reporting API, Audit API.

About ISO 27001

ISO 27001 is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes and data centers serving Google Apps for Business.

Our compliance with the ISO 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 member.

SSAE 16 / ISAE 3402 / SAS 70 Audit

Auditors: Grant Thornton LLP

Services Covered: GMail, Google Talk, Google Calendar, Google Docs (documents, spreadsheets, presentations), Google Sites, Google Start Page (iGoogle), Control Panel (CPanel), Google App Engine, Google Apps Script, Google Storage for Developers, and Google Postini Services – Google Message Security and Google Message Discovery.

Report Types: SSAE16/ISAE 3402 Type II and SAS 70 Type II

About SSAE 16 / ISAE 3204 / SAS 70

SSAE 16 Type II – Statement on Standards for Attestation Engagements (SSAE) No. 16, is an attestation standard issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). ISAE 3402 is the new globally recognized standard for assurance reporting on service organizations and will be more relevant to our international customers. SSAE 16 and ISAE 3402 replace SA70.

Major Control Objectives and Control Activities Covered

Logical security controls provide reasonable assurance that logical access to production systems is restricted to authorized individuals.
Privacy controls provide reasonable assurance that Google has implemented policies and procedures addressing the privacy of customer data.
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 incidents are identified, analyzed, and tracked for resolution.
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: Grant Thornton issued an unqualified opinion with zero exceptions on any control objectives or control activities during the period for all reports.