

Google Cloud Platform (GCP) Audit Program



CONTENTS

4	Google Cloud Platform Audit Program
	4 / Audit Objective
	4 / Audit Scope
	4 / Business Impact and Risk
	4 / Minimum Audit Skills
	4 / Testing Steps
5	Acknowledgments

ABSTRACT

As many companies undergo digital innovation and transformation, optimize global workforce access to productivity tools and shift business operations to hybrid, single cloud or multicloud environments, auditors must be prepared with a framework to understand and assess risk across various enterprise cloud technologies. ISACA has been an early leader in developing auditing templates for the widely used enterprise cloud services providers: Microsoft Azure and Amazon Web Services (AWS). With the continued growth and adoption of the Google Cloud Platform (GCP), which is now the third-largest provider of cloud services, ISACA has developed an audit program that helps auditors assess and test the internal control adequacy and effectiveness of GCP services, adding to the library of frameworks that exists for the two other major cloud providers.

Once at the forefront of emerging technology, most enterprises and government entities have moved some level of critical services either partially or entirely to the cloud. This allows them to take advantage of the availability, flexibility and scalability of cloud platforms and services. Although the classification of “cloud computing” necessitates having certain characteristics, each cloud provider differentiates itself with the types of services provided, the terminology it uses, and the enhancements and innovations offered. ISACA created the GCP Audit Program to help auditors develop an audit program that caters to the uniqueness of GCP while effectively assessing an enterprise cloud environment for adherence to organizational risk and compliance objectives.¹

¹ Google Cloud, “State of Cloud Threat Detection and Response Report,” March 2023, https://services.google.com/fh/files/misc/gcat_cloud_dr_survey_report_2023.pdf

Google Cloud Platform Audit Program

Audit Objective

This audit program assists IT auditors in performing operational and compliance assessments for GCP designed to address both general cloud computing attributes and specialized Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and even Identity-as-a-Service (IDaaS) services. The program will aid IT auditors in evaluating whether the enterprise has configured and enabled GCP services in a way that securely supports the enterprise's business, operational and compliance goals.

Audit Scope

The audit program covers the following areas:

- Governance
- Network configuration and management
- Resource configuration and management
- Data security and integrity
- Security incident response
- Business continuity and resiliency
- Security logging and monitoring
- Identity and access management

Business Impact and Risk

In general, one of the most significant areas of risk within a cloud environment is the prevalence of misconfigurations and misunderstandings about shared cloud responsibilities as enterprises tailor and scale services to meet the needs of their operations. In particular, for GCP, it is vitally important to understand concepts around identity and access management, the Organization/Project/Folder structure, the impacts of

inheritance and hierarchy on access and permissions and the enablement/disablement of logging options. Not understanding these can lead to missing areas of assessment as well as an increased likelihood that risk goes undetected until an incident occurs. Most security professionals believe maintaining security within a cloud environment is more difficult and involves greater risk than an on-premises environment.² Given the dynamic nature of the cloud and the pace and frequency at which cloud services are evolving—with newly added services, new features of existing services, deprecation of services and newly detected vulnerabilities—security professionals' concerns regarding the business impact of risk are well-founded.

Minimum Audit Skills

The GCP Audit Program assumes that auditors exercise due professional care and possess professional competencies culminating in the proficiency to conduct an audit inclusive of cloud computing environments. ITAF Standard 1005 requires that the auditor exercise due diligence and professional care; professional skepticism and effective communication should be maintained throughout the course of an audit. ITAF Standard 1006 also requires that the auditor have professional competence and technical skill in the areas under assessment³. This expectation is particularly relevant to auditors who do not hold the CISA (or another appropriate) certification designation.

Testing Steps

Refer to the accompanying spreadsheet file for guidance on testing GCP services.

² Ibid.

³ ISACA, *IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition, 2020*

Acknowledgments

ISACA would like to recognize:

Lead Developer

Shinesa Cambric

CISA, CCSP, CISSP
USA

Expert Reviewers

Ibrahim Sulaiman Alnamlah

CISA, COBIT2019, ISO/IEC27001LA,
ITILV4
Saudi Arabia

R.V. Raghu

CISA, CRISC, CCSK
India

Naveen Rajani

CISA, CISSP, ITIL
Germany

Ignatius Ravi

CISA
USA

James Wallmuller

CISA, CRISC, CDPSE
USA

Board of Directors

Pamela Nigro, Chair

CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision,
USA

John De Santis, Vice-Chair

Former Chairman and Chief Executive
Officer, HyTrust, Inc., USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC
Chief Information Security Officer, Data
Privacy Officer, Doodle GmbH, France

Gabriela Hernandez-Cardoso

NACD.DC
Independent Board Member, Mexico

Maureen O'Connell

NACD.DC
Board Chair, Acacia Research (NASDAQ),
Former Chief Financial Officer and Chief
Administration Officer, Scholastic, Inc.,
USA

Veronica Rose

CISA, CDPSE
Senior Information Systems Auditor–
Advisory Consulting, KPMG Uganda,
Founder, Encrypt Africa, Kenya

Gerrard Schmid

Former President and Chief Executive
Officer, Diebold Nixdorf, USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd.,
Israel

Erik Prusch

Chief Executive Officer, ISACA, USA

Gregory Touhill

ISACA Board Chair, 2021-2022
CISM, CISSP
Director, CERT Center,
Carnegie Mellon University, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City
Bancorp, USA

Brennan P. Baybeck

ISACA Board Chair, 2019-2020
CISA, CISM, CRISC, CISSP
Senior Vice President and Chief
Information Security Officer for
Customer Services, Oracle Corporation,
USA

Rob Clyde

ISACA Board Chair, 2018-2019
CISM, NACD.DC
Independent Director, Titus, Executive
Chair, White Cloud Security, Managing
Director, Clyde Consulting LLC, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

Disclaimer

ISACA has designed and created *Google Cloud Platform (GCP) Audit Program* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2023 ISACA. All rights reserved.



1700 E. Golf Road, Suite 400

Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: [support.isaca.org](mailto:support@isaca.org)

Website: www.isaca.org

Provide

Feedback:

<https://www.isaca.org/google-cloud-platform-audit-program>

Participate in the ISACA Online

Forums: <https://engage.isaca.org/onlineforums>

Twitter: [www.twitter.com/ISACANews](https://twitter.com/ISACANews)

LinkedIn: www.linkedin.com/company/isaca

Facebook: www.facebook.com/ISACAGlobal

Instagram: www.instagram.com/isacanews/