



Vendor Control Assessment

Vendor: Google

Service / Product: Browser, Bucket, GCP, and SQL

Assessment: Riskonami

Assessment date: 2026-10-01

Assessment version: v2

Organizational contact: Musmato

Questionnaire answers: absorbed

1. Vendor Assessment Statement

This assessment identifies the security and risk-control requirements applicable to **Google** for the delivery of **Browser, Bucket, GCP, and SQL** within **GCP, Public**. Riskonami identified **35** controls for which vendor assurance is required. Based on the assurance currently available, **28** requirements are satisfied, **0** are partially satisfied and **7** remain unresolved. The current assurance position is **assurance partially satisfied** in relation to the organization's stated risk requirements. The vendor may demonstrate implementation through suitable evidence, including relevant certification where the certification scope adequately covers the requirement, or through other evidence specified in this report.

2. Vendor and Service Scope

2.1 Vendor

Google

2.2 Service / Product

Browser, Bucket, GCP, and SQL

2.3 Assessment Boundary

GCP, Public

3. Assurance Context

- We do not know whether backup and restore is in place for Bucket, so it is treated as no protection. an external attacker could interrupt or degrade the service. Current risk medium.
- We do not know whether backup and restore is in place for SQL, so it is treated as no protection. an external attacker could interrupt or degrade the service. Current risk medium.
- We do not know whether supplier assurance is in place for Bucket, so it is treated as no protection. a supplier or third party could abuse a supplier or third-party path into this system. Current risk high.
- We do not know whether logging is in place for Bucket, so it is treated as no protection. an external attacker could go unnoticed after accessing data or systems. Current risk high.

- We do not know whether authentication is in place for SQL, so it is treated as no protection. an external attacker could guess, steal, or bypass a login. Current risk high.
- We do not know whether authorization is in place for SQL, so it is treated as no protection. an external attacker could act with more access than they should have. Current risk high.
- We do not know whether data-at-rest protection is in place for SQL, so it is treated as no protection. an external attacker could read stored data. Current risk high.
- We do not know whether logging is in place for SQL, so it is treated as no protection. an external attacker could go unnoticed after accessing data or systems. Current risk high.
- We do not know whether supplier assurance is in place for SQL, so it is treated as no protection. a supplier or third party could abuse a supplier or third-party path into this system. Current risk high.
- We do not know whether supplier assurance is in place for GCP, so it is treated as no protection. a supplier or third party could abuse a supplier or third-party path into this system. Current risk high.

4. Applicable Vendor Controls

Each row names the ISO control and **what this control requires**.

Control	What this control requires	Component	Implementation	Assurance
5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	Bucket	implemented	supplier_relationship
5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	Bucket	implemented	supplier_agreement
5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	Bucket	implemented	supply_chain
5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	Bucket	implemented	supplier_monitoring
5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	Bucket	implemented	resilience
5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	Bucket	implemented	resilience

Control	What this control requires	Component	Implementation	Assurance
8.13 Information backup	Take copies of information, software and systems, and test restoration, according to an agreed backup policy.	Bucket	implemented	resilience
8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	Bucket	implemented	resilience
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Bucket	implemented	logging
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Bucket	implemented	logging
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Bucket	implemented	logging
5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	GCP	implemented	supplier_relationship
5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	GCP	implemented	supplier_agreement
5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	GCP	implemented	supply_chain
5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	GCP	implemented	supplier_monitoring
5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	SQL	implemented	authorization

Control	What this control requires	Component	Implementation	Assurance
5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	SQL	implemented	authentication
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	SQL	unknown	authorization
5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	SQL	unknown	supplier_relationship
5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	SQL	unknown	supplier_agreement
5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	SQL	unknown	supply_chain
5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	SQL	unknown	supplier_monitoring
5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	SQL	unknown	resilience
5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	SQL	unknown	resilience
8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that do not need the real values cannot see them.	SQL	implemented	data_at_rest
8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	SQL	implemented	data_at_rest
8.13 Information backup	Take copies of information, software and systems, and test	SQL	implemented	resilience

Control	What this control requires	Component	Implementation	Assurance
	restoration, according to an agreed backup policy.			
8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	SQL	implemented	resilience
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	SQL	implemented	logging
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	SQL	implemented	logging
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	SQL	implemented	logging
8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	SQL	implemented	authorization
8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of the information.	SQL	implemented	data_at_rest
8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	SQL	implemented	authorization
8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	SQL	implemented	authentication

5. Acceptable Assurance and Evidence

The vendor may satisfy an applicable control requirement using one or more forms of evidence accepted by the organization. Evidence must relate to the service and scope assessed in this report.

Suitable evidence may include a certification whose scope covers the listed requirement, or other evidence accepted by the organisation.

A certification, audit report or attestation does not automatically satisfy a control unless its scope and coverage are sufficient for the specific requirement.

6. Outstanding Vendor Requirements

Control	What this control requires	Component	Implementation
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	SQL	unknown
5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	SQL	unknown
5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	SQL	unknown
5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	SQL	unknown
5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	SQL	unknown
5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	SQL	unknown
5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	SQL	unknown

7. Exceptions, Alternative Controls and Compensating Controls

None recorded.

8. Vendor Assurance Outcome

Current assurance position: assurance partially satisfied

Outstanding requirements: 7

Assessment status: assurance partially satisfied

Satisfied	Partial	Outstanding
28	0	7

Generated by Riskonami from assessment data version v2. This vendor-facing report contains only the risk context and control requirements approved for external disclosure. Internal threat intelligence, architecture details and unrelated organizational risk information are intentionally excluded.