



Overall Risk Assessment Report

Assessment: Riskonami

System / Service: Riskonami

Assessment date: 2026-10-01

Assessment version: v2

Prepared for: Management and engineering

Risk owner: Musmato

1. Combined Assessment

This overall view combines this organisation's assessed residual with **accepted** vendor-review answers. Unanswered or uncured vendor implementation stays transferred and is not treated as this organisation's residual. Vendor-reviewed rows are labelled as vendor review.

Management attention is required for:

- Supplier assurance on Bucket
- Authentication on SQL
- Supplier assurance on GCP

2. Assessment Context

2.1 Objectives

The objective of the assessment is to identify the risk associated with a specific application and provide Assurance system management

2.2 Scope

In scope

- Server (application)

External dependency (third party)

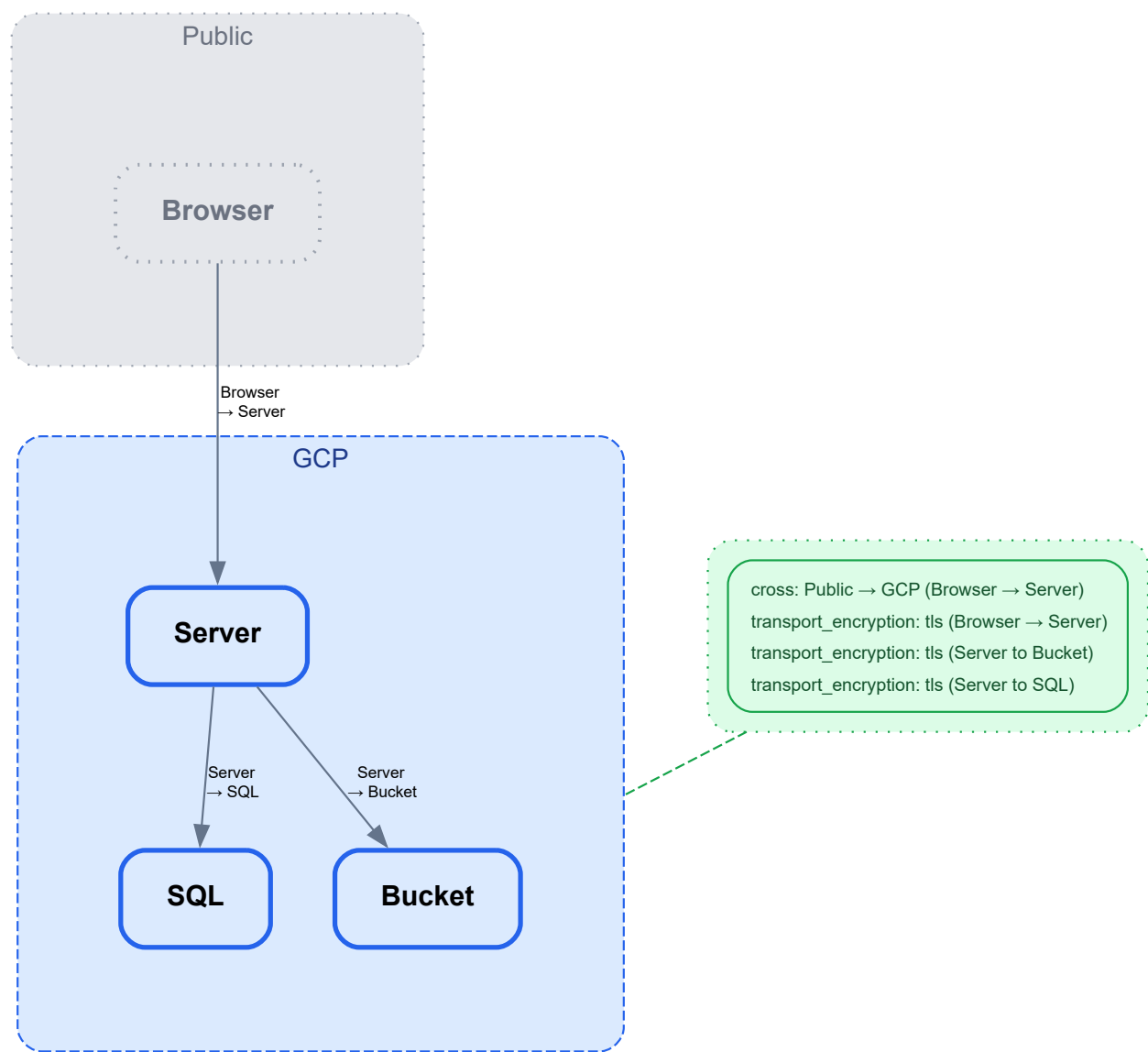
- GCP (trust zone) — Google
- Bucket (application) — Google
- SQL (application) — Google

Out of scope (tracked, not residual)

- Public (trust zone) — ISP
- Browser (application) — Google

Access hop. Residual on a connection this organisation implements between an out-of-scope presence (for example a browser or unmanaged client) and an in-scope system is labelled Riskonami (access hop). It is not a risk on the out-of-scope node. The architecture diagram still shows the pair names (for example Browser → Riskonami).

2.3 System diagram



Security facts

GCP

- Boundary crossing: Public → GCP (Browser → Server)
- Transport encryption: tls (Browser → Server)
- Transport encryption: tls (Server to Bucket)
- Transport encryption: tls (Server to SQL)

3. Overall Risk Position

Overall residual risk	Risk appetite position
high	outside risk appetite

Combined residual: high

Risk appetite position: outside risk appetite

4. Material Risks

Why numbers are residual bands (0 very low ... 5 extreme). Negative is remaining residual after this control. Positive is how many bands this control removed from the unprotected position. Individual measures are not scored separately: stacking is not additive.

Material risks below are this organisation's residual plus accepted vendor-review rows, with party and source on each row. Unaccepted vendor residual stays in Vendor responsibility and is not in the combined residual.

Risk	Component	Party	Source	Current residual	Decision	Why
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.	Bucket	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown supplier assurance state; not in place: Cloud/SaaS assurance: contract, SOC2/ISO evidence, shared-responsibility review; Security schedule, right-to-audit and incident-notice in the contract; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 5.19 Information security in supplier relationships; 5.20 Addressing information security within supplier agreements; 5.21 Managing information security in the ICT supply chain; and 1 more.
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.	Bucket	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown logging state; not in place: Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync; unknown protection scored as no protection

Risk	Component	Party	Source	Current residual	Decision	Why
						Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization.
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.	SQL	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authentication state; not in place: Phishing-resistant MFA (passkeys / FIDO2); Multi-factor authentication (on passwords or single sign-on); Single sign-on (OAuth 2.0, OIDC, or SAML) without MFA; Individually allocated accounts (not shared or generic logins); Secret policy enforced (ISO 5.17: allocate, protect, change); Unprotected passwords or keys, no secret-handling policy; Automated joiner-mover-leaver provisioning for the application; Non-retained API credentials (short-lived or workload identity); Encrypted, vaulted and rotated API keys; Partially protected API keys; Cleartext or embedded API keys; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.5 Secure authentication; 5.17 Authentication information.
We do not know whether authorization is in place for SQL, so it is treated as no protection. An external attacker	SQL	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authorization state; not in place: Role-based or attribute-based access with

Risk	Component	Party	Source	Current residual	Decision	Why
could act with more access than they should have. Current risk high.						least privilege; Default-deny authorisation at the object or API; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more.
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.	SQL	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown data-at-rest protection state; not in place: Transparent data encryption and access controls on the database; Volume or object-store encryption with managed keys; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.24 Use of cryptography; 8.11 Data masking; 8.12 Data leakage prevention.
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.	SQL	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown logging state; not in place: Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring

Risk	Component	Party	Source	Current residual	Decision	Why
						activities; 8.17 Clock synchronization.
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.	GCP	Google	Vendor review — Google	high	transfer	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown supplier assurance state; not in place: Cloud/SaaS assurance: contract, SOC2/ISO evidence, shared-responsibility review; Security schedule, right-to-audit and incident-notice in the contract; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 5.19 Information security in supplier relationships; 5.20 Addressing information security within supplier agreements; 5.21 Managing information security in the ICT supply chain; and 1 more.
We do not know whether input validation is in place for Server, so it is treated as no protection. An external attacker could inject or alter submitted data. Current risk high.	Server	Organisation	This organisation	high	mitigate	Negative -3 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown input validation state; not in place: Allow-list validation and output encoding at the trust boundary; Edge filtering (WAF / API schema) in front of this input; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.26 Application security requirements.
We do not know whether backup and restore is in place for Bucket,	Bucket	Google	Vendor review — Google	high	transfer	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength,

Risk	Component	Party	Source	Current residual	Decision	Why
so it is treated as no protection. An external attacker could interrupt or degrade the service. Current risk medium.						initiation possible; unknown backup and restore state; not in place: Backup and recovery tested for RPO/RTO; Redundancy or failover matching the availability need; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.13 Information backup; 8.14 Redundancy of information processing facilities; 5.29 Information security during disruption; and 1 more.
Logging for Server → SQL is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server → SQL	Organisation	This organisation	medium	mitigate	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown logging state Positive +1 adequate protection reduced residual; in place: Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization.
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.	SQL	Google	Vendor review — Google	high	transfer	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown backup and restore state; not in place: Backup and recovery tested for RPO/RTO; Redundancy or failover matching the availability need; unknown protection scored as no protection Positive +0 nothing recorded reduced this residual

Risk	Component	Party	Source	Current residual	Decision	Why
						Relevant ISO (not a cause): 8.13 Information backup; 8.14 Redundancy of information processing facilities; 5.29 Information security during disruption; and 1 more.
Platform hardening for the delivery platform is no protection. An environmental or infrastructure failure could disrupt the hosting or platform layer. Current risk medium.	Platform / delivery	Organisation	This organisation	medium	mitigate	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown platform hardening state; not in place: Secure configuration and hardening baseline; Vulnerability management and patch programme; no protection kept residual up Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 5.23 Information security for use of cloud services; 5.29 Information security during disruption; 5.30 ICT readiness for business continuity; and 12 more.
Logging for Server → Bucket is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server → Bucket	Organisation	This organisation	medium	accept	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown logging state Positive +1 adequate protection reduced residual; in place: Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization.
Boundary protection for Server (access hop) is adequate protection. An external attacker	Server (access hop)	Organisation	This organisation	medium	accept	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown boundary protection state;

Risk	Component	Party	Source	Current residual	Decision	Why
could cross a trust boundary they should not. Current risk medium.						not in place: Stateful / next-generation firewall with default-deny on this crossing; Network segmentation / micro-segmentation for this crossing; Reverse proxy or API gateway on this crossing; WAF with OWASP baseline rules and tuned exceptions Positive +1 adequate protection reduced residual; in place: Packet filtering firewall or network ACL on this crossing Relevant ISO (not a cause): 8.22 Segregation of networks.
Logging for Server (access hop) is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server (access hop)	Organisation	This organisation	medium	mitigate	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown logging state Positive +1 adequate protection reduced residual; in place: Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization.
Logging for Server is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server	Organisation	This organisation	medium	mitigate	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown logging state Positive +1 adequate protection reduced residual; in place: Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring

Risk	Component	Party	Source	Current residual	Decision	Why
						activities; 8.17 Clock synchronization.
Secure operations and change for Server is no protection. Accidental misuse or error could change how the service is run, by mistake or misuse. Current risk medium.	Server	Organisation	This organisation	medium	mitigate	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation rare; unknown secure operations and change state; not in place: Secure development and change-control programme; Malware protection and monitoring on operational components; no protection kept residual up Positive +0 nothing recorded reduced this residual Relevant ISO (not a cause): 8.4 Access to source code; 8.25 Secure development life cycle; 8.27 Secure system architecture and engineering principles; and 6 more.
Secrets protection for Server is adequate protection. An external attacker could obtain keys or credentials. Current risk medium.	Server	Organisation	This organisation	medium	accept	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown secrets protection state Positive +1 adequate protection reduced residual; in place: Central secrets manager with audit logging; No long-lived secrets in code, images or tickets Relevant ISO (not a cause): 5.17 Authentication information.
Transport protection for Server → SQL is strong protection. An external attacker could read or alter data in transit. Current risk low.	Server → SQL	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; medium strength, initiation possible; not in place: Mutual TLS between services on this hop Positive +2 strong protection reduced residual; in place: TLS 1.2+ for all external and cross-zone flows

Risk	Component	Party	Source	Current residual	Decision	Why
						Relevant ISO (not a cause): 8.24 Use of cryptography; 5.14 Information transfer; 8.20 Network security.
Authentication for Server → SQL is strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	Server → SQL	Organisation	This organisation	low	accept	Negative –1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authentication state; not in place: Phishing-resistant MFA (passkeys / FIDO2); Multi-factor authentication (on passwords or single sign-on); Single sign-on (OAuth 2.0, OIDC, or SAML) without MFA; Individually allocated accounts (not shared or generic logins); Secret policy enforced (ISO 5.17: allocate, protect, change); Unprotected passwords or keys, no secret-handling policy; Automated joiner-mover-leaver provisioning for the application; Encrypted, vaulted and rotated API keys; Partially protected API keys; Cleartext or embedded API keys Positive +2 strong protection reduced residual; in place: Non-retained API credentials (short-lived or workload identity) Relevant ISO (not a cause): 8.5 Secure authentication; 5.17 Authentication information.
Authorization for Server → SQL is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server → SQL	Organisation	This organisation	low	accept	Negative –1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authorization state Positive +2 strong protection reduced residual; in place: Role-based or attribute-based access with least privilege; Default-deny authorisation at the object or API

Risk	Component	Party	Source	Current residual	Decision	Why
						Relevant ISO (not a cause): 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more.
Information security governance for this organisation is strong protection. Someone inside the organisation could socially engineer staff or processes. Current risk low.	Organisation	Organisation	This organisation	low	accept	Negative –1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown information security governance state Positive +2 strong protection reduced residual; in place: Information security policy and governance programme; Risk assessment and treatment programme; Roles, responsibilities and segregation of duties programme Relevant ISO (not a cause): 5.1 Policies for information security; 5.2 Information security roles and responsibilities; 5.3 Segregation of duties; and 32 more.
Transport protection for Server → Bucket is strong protection. An external attacker could read or alter data in transit. Current risk low.	Server → Bucket	Organisation	This organisation	low	accept	Negative –1 CIA confidentiality high, integrity high, availability medium; medium strength, initiation possible Positive +2 strong protection reduced residual; in place: TLS 1.2+ for all external and cross-zone flows; Mutual TLS between services on this hop Relevant ISO (not a cause): 8.24 Use of cryptography; 5.14 Information transfer; 8.20 Network security.
Authentication for Server → Bucket is strong protection. An external attacker could guess, steal, or bypass a	Server → Bucket	Organisation	This organisation	low	accept	Negative –1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authentication state; not in place: Phishing-resistant MFA (passkeys / FIDO2);

Risk	Component	Party	Source	Current residual	Decision	Why
login. Current risk low.						Multi-factor authentication (on passwords or single sign-on); Single sign-on (OAuth 2.0, OIDC, or SAML) without MFA; Individually allocated accounts (not shared or generic logins); Secret policy enforced (ISO 5.17: allocate, protect, change); Unprotected passwords or keys, no secret-handling policy; Automated joiner-mover-leaver provisioning for the application; Encrypted, vaulted and rotated API keys; Partially protected API keys; Cleartext or embedded API keys Positive +2 strong protection reduced residual; in place: Non-retained API credentials (short-lived or workload identity) Relevant ISO (not a cause): 8.5 Secure authentication; 5.17 Authentication information.
Authorization for Server → Bucket is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server → Bucket	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authorization state Positive +2 strong protection reduced residual; in place: Role-based or attribute-based access with least privilege; Default-deny authorisation at the object or API Relevant ISO (not a cause): 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more.
Transport protection for Server (access hop) is strong protection. An external attacker could read or	Server (access hop)	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; medium strength, initiation possible; not in place: Mutual TLS between services on this hop

Risk	Component	Party	Source	Current residual	Decision	Why
alter data in transit. Current risk low.						Positive +2 strong protection reduced residual; in place: TLS 1.2+ for all external and cross-zone flows Relevant ISO (not a cause): 8.24 Use of cryptography; 5.14 Information transfer; 8.20 Network security.
Authentication for Server (access hop) is strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	Server (access hop)	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authentication state; not in place: Multi-factor authentication (on passwords or single sign-on); Individually allocated accounts (not shared or generic logins); Secret policy enforced (ISO 5.17: allocate, protect, change); Unprotected passwords or keys, no secret-handling policy; Automated joiner-mover-leaver provisioning for the application; Non-retained API credentials (short-lived or workload identity); Encrypted, vaulted and rotated API keys; Partially protected API keys; Cleartext or embedded API keys Positive +2 strong protection reduced residual; in place: Phishing-resistant MFA (passkeys / FIDO2); Single sign-on (OAuth 2.0, OIDC, or SAML) without MFA Relevant ISO (not a cause): 8.5 Secure authentication; 5.17 Authentication information.
Authorization for Server (access hop) is strong protection. An external attacker could act with	Server (access hop)	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authorization state

Risk	Component	Party	Source	Current residual	Decision	Why
more access than they should have. Current risk low.						Positive +2 strong protection reduced residual; in place: Role-based or attribute-based access with least privilege; Default-deny authorisation at the object or API Relevant ISO (not a cause): 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more.
Input validation for Server (access hop) is strong protection. An external attacker could inject or alter submitted data. Current risk low.	Server (access hop)	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown input validation state; not in place: Edge filtering (WAF / API schema) in front of this input Positive +2 strong protection reduced residual; in place: Allow-list validation and output encoding at the trust boundary Relevant ISO (not a cause): 8.26 Application security requirements.
Authorization for Server is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown authorization state Positive +2 strong protection reduced residual; in place: Role-based or attribute-based access with least privilege; Default-deny authorisation at the object or API Relevant ISO (not a cause): 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more.
Data-at-rest protection for Server is strong protection. An	Server	Organisation	This organisation	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength,

Risk	Component	Party	Source	Current residual	Decision	Why
external attacker could read stored data. Current risk low.						initiation possible; unknown data-at-rest protection state Positive +2 strong protection reduced residual; in place: Transparent data encryption and access controls on the database; Volume or object-store encryption with managed keys Relevant ISO (not a cause): 8.24 Use of cryptography; 8.11 Data masking; 8.12 Data leakage prevention.

5. Vendor responsibility

This organisational view does not score vendor residual. Each row is a named partner, how many controls they own on this snapshot, and that share of partner-owned controls (weight). Outstanding items and transferred risks stay in that partner's vendor assessment download.

Vendor	Components	Partner-owned controls	Weight	Outstanding	Transferred risks	Assurance
Google	Browser, Bucket, GCP, SQL	35	100%	7	10	assurance partially satisfied
ISP	Public	0	0%	0	0	no partner-owned controls recorded

Vendor	Component	Risk	Current residual	Decision
Google	Bucket	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.	medium	transfer
Google	SQL	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.	medium	transfer
Google	Bucket	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.	high	transfer
Google	Bucket	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.	high	transfer
Google	SQL	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.	high	transfer

Vendor	Component	Risk	Current residual	Decision
Google	SQL	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.	high	transfer
Google	SQL	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.	high	transfer
Google	SQL	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.	high	transfer
Google	SQL	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.	high	transfer
Google	GCP	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.	high	transfer

6. Risk Treatment and Management Actions

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
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.	Bucket	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering supplier.	M
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.	Bucket	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering logging.	M
We do not know whether authentication is in place for SQL, so it is treated as no protection. An external	SQL	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering authentication.	M

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
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.	SQL	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering authorization.	M
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.	SQL	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering data_at_rest.	M
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.	SQL	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering logging.	M
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.	GCP	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering supplier.	M
We do not know whether input validation is in place for Server, so it is treated as no protection. An external attacker could	Server	Security Engineer (organisation)	mitigate	remediation	Remediate input validation weakness; Allow-list validation and output encoding at the trust boundary; Edge filtering (WAF /	M

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
inject or alter submitted data. Current risk high.					API schema) in front of this input	
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.	Bucket	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering resilience.	M
Logging for Server → SQL is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server → SQL	Security Engineer (organisation)	mitigate	remediation	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync	M
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.	SQL	Google (supplier)	transfer	transfer	Commission a vendor assessment for Google covering resilience.	M
Platform hardening for the delivery platform is no protection. An environmental or infrastructure failure could disrupt the hosting or platform layer. Current risk medium.	Platform / delivery	Security Engineer (unknown)	mitigate	remediation	Remediate platform hardening weakness; Secure configuration and hardening baseline; Vulnerability management and patch programme	M
Logging for Server → Bucket is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server → Bucket	Google (organisation)	accept	—	No treatment — accepted at P7.	S

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
Boundary protection for Server (access hop) is adequate protection. An external attacker could cross a trust boundary they should not. Current risk medium.	Server (access hop)	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Logging for Server (access hop) is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server (access hop)	Security Engineer (organisation)	mitigate	remediation	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync	M
Logging for Server is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server	Security Engineer (organisation)	mitigate	remediation	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync	M
Secure operations and change for Server is no protection. Accidental misuse or error could change how the service is run, by mistake or misuse. Current risk medium.	Server	Security Engineer (organisation)	mitigate	remediation	Remediate secure operations and change weakness; Secure development and change-control programme; Malware protection and monitoring on operational components	M
Secrets protection for Server is adequate protection. An external attacker could obtain keys or credentials. Current risk medium.	Server	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Transport protection for Server → SQL is strong protection. An external attacker could read or alter data in transit. Current risk low.	Server → SQL	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Authentication for Server → SQL is strong	Server → SQL	Security Engineer	accept	—	No treatment — accepted at P7.	S

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
protection. An external attacker could guess, steal, or bypass a login. Current risk low.		(organisation)				
Authorization for Server → SQL is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server → SQL	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Information security governance for this organisation is strong protection. Someone inside the organisation could socially engineer staff or processes. Current risk low.	Organisation	unknown	accept	—	No treatment — accepted at P7.	S
Transport protection for Server → Bucket is strong protection. An external attacker could read or alter data in transit. Current risk low.	Server → Bucket	Google (organisation)	accept	—	No treatment — accepted at P7.	S
Authentication for Server → Bucket is strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	Server → Bucket	Google (organisation)	accept	—	No treatment — accepted at P7.	S
Authorization for Server → Bucket is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server → Bucket	Google (organisation)	accept	—	No treatment — accepted at P7.	S
Transport protection for Server (access hop) is strong protection. An external attacker could read or alter data in transit. Current risk low.	Server (access hop)	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Authentication for Server (access hop) is	Server (access hop)	Security Engineer	accept	—	No treatment — accepted at P7.	S

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.		(organisation)				
Authorization for Server (access hop) is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server (access hop)	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Input validation for Server (access hop) is strong protection. An external attacker could inject or alter submitted data. Current risk low.	Server (access hop)	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Authorization for Server is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
Data-at-rest protection for Server is strong protection. An external attacker could read stored data. Current risk low.	Server	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S

Decisions or Actions Required

Task	Owner	Effort	Component	Control type	Suggested remediation
Establish contractual security requirements with third party	Google	M	Bucket	Logging	Commission a vendor assessment for Google covering logging.
Establish contractual security requirements with third party	Google	M	Bucket	Backup and restore	Commission a vendor assessment for Google covering resilience.
Establish contractual security requirements with third party	Google	M	Bucket	Supplier assurance	Commission a vendor assessment for Google covering supplier.

Task	Owner	Effort	Component	Control type	Suggested remediation
Establish contractual security requirements with third party	Google	M	SQL	Authorization	Commission a vendor assessment for Google covering authorization.
Establish contractual security requirements with third party	Google	M	SQL	Data-at-rest protection	Commission a vendor assessment for Google covering data_at_rest.
Establish contractual security requirements with third party	Google	M	SQL	Logging	Commission a vendor assessment for Google covering logging.
Establish contractual security requirements with third party	Google	M	SQL	Backup and restore	Commission a vendor assessment for Google covering resilience.
Establish contractual security requirements with third party	Google	M	SQL	Supplier assurance	Commission a vendor assessment for Google covering supplier.
Establish contractual security requirements with third party	Google	M	SQL	Authentication	Commission a vendor assessment for Google covering authentication.
Establish contractual security requirements with third party	Google	M	GCP	Supplier assurance	Commission a vendor assessment for Google covering supplier.
Remediate logging weakness	Security Engineer	M	Server → SQL	Logging	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync
Remediate platform hardening weakness	Security Engineer	M	Platform / delivery	Platform hardening	Remediate platform hardening weakness; Secure configuration and hardening baseline; Vulnerability management and patch programme
Remediate logging weakness	Security Engineer	M	Server (access hop)	Logging	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync
Remediate input validation weakness	Security Engineer	M	Server	Input validation	Remediate input validation weakness; Allow-list validation and output encoding at the trust boundary; Edge

Task	Owner	Effort	Component	Control type	Suggested remediation
					filtering (WAF / API schema) in front of this input
Remediate logging weakness	Security Engineer	M	Server	Logging	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync
Remediate secure operations and change weakness	Security Engineer	M	Server	Secure operations and change	Remediate secure operations and change weakness; Secure development and change-control programme; Malware protection and monitoring on operational components

7. Conclusion

The combined residual risk position for **Riskonami** is **high**, built from organisational P5 answers and accepted vendor reviews only.

Generated by Riskonami from assessment data version v2. Accepted vendor answers are labelled vendor review and do not replace the organisational walk.