



Executive 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. Executive Assessment

This assessment evaluates **Riskonami**. It is positioned against the stated objective: the objective of the assessment is to identify the risk associated with a specific application and provide Assurance system management. It covers the in-scope components listed in Section 2.2. The current overall residual risk is **high** against a declared risk appetite of **Company can tolerate low risk**. The resulting appetite position is **outside risk appetite**. The assessment identified **22** material risks, **26** open control gaps and **14** material threat scenarios.

Management attention is required for:

- Input validation on Server
- Logging on Server → Bucket
- Boundary protection on Server (access hop)

Any material assumptions, limitations or exceptional circumstances are recorded in Section 7.

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)

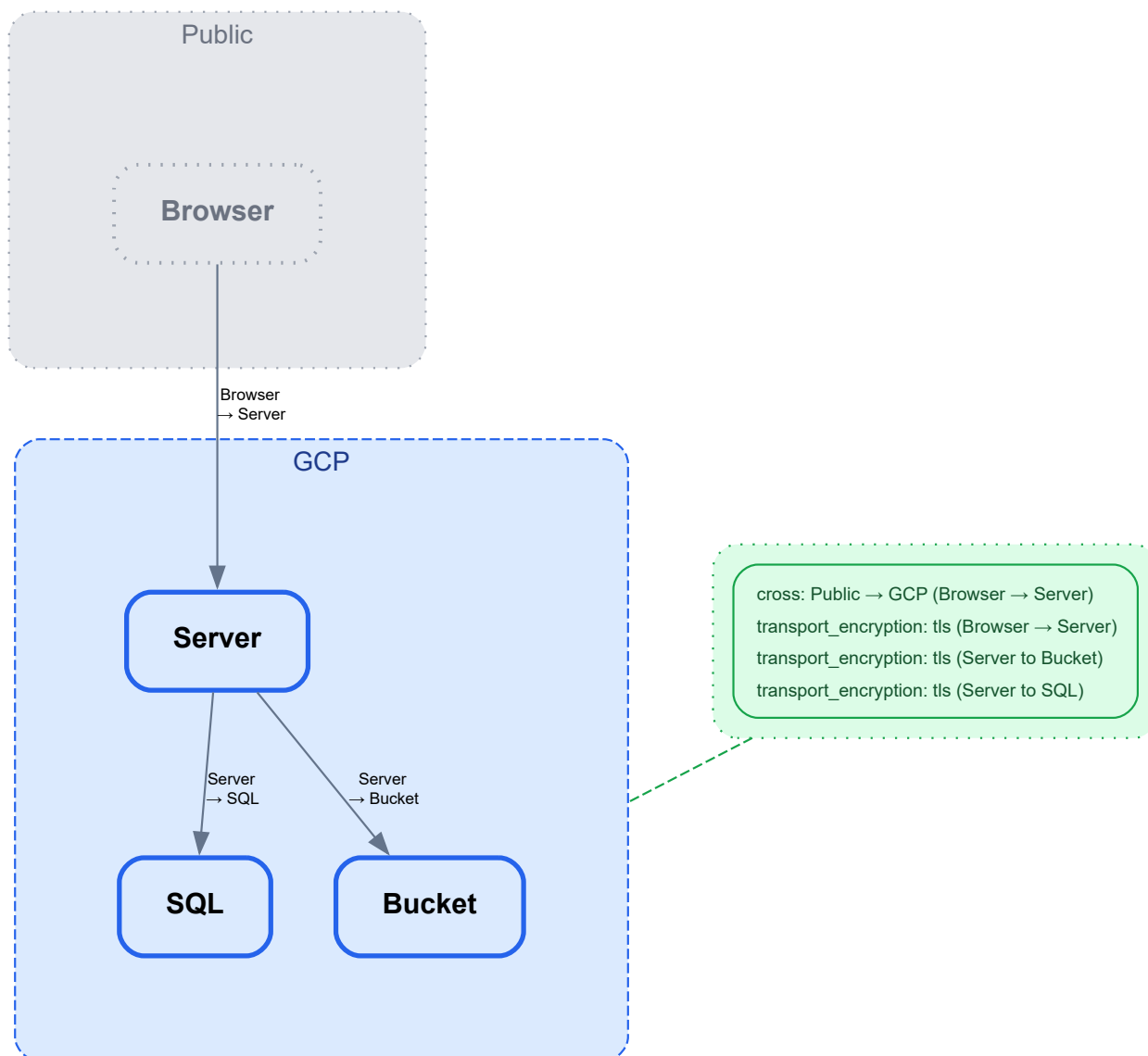
- GCP (trust zone) — Google
- Bucket (application) — Google
- SQL (application) — Google

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)

2.4 Intended Audience

2.5 Risk Appetite

Company can tolerate low risk

3. Overall Risk Position

Overall residual risk	Risk appetite position
high	outside risk appetite

Risk appetite position: outside risk appetite

Deterministic rationale: Residual high against a maximum accepted residual of low.

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.

Suggested remediation, including labeled AI advice where generated, is in Section 6.

Risk	Component	Current residual	Decision	Why
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	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.
Logging for Server → SQL is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server → SQL	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.
Platform hardening for the delivery platform is no protection. An environmental or infrastructure failure could disrupt the hosting or platform	Platform / delivery	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

Risk	Component	Current residual	Decision	Why
layer. Current risk medium.				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	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 could cross a trust boundary they should not. Current risk medium.	Server (access hop)	medium	accept	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown boundary protection state; 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)	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	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.
Secure operations and change for Server is no protection. Accidental misuse or error could change how the service	Server	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

Risk	Component	Current residual	Decision	Why
is run, by mistake or misuse. Current risk medium.				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	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	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 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	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	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	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	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	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 login. Current risk low.	Server → Bucket	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.

Risk	Component	Current residual	Decision	Why
Authorization for Server → Bucket is strong protection. An external attacker could act with more access than they should have. Current risk low.	Server → Bucket	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 alter data in transit. Current risk low.	Server (access hop)	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 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)	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 more access than they should have. Current risk low.	Server (access hop)	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.
Input validation for Server (access hop) is strong protection. An external attacker could	Server (access hop)	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown input validation state; not in

Risk	Component	Current residual	Decision	Why
inject or alter submitted data. Current risk low.				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	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 external attacker could read stored data. Current risk low.	Server	low	accept	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, 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. Threat Posture

5.1 Threat scenarios

Why is the threat-pack cause (who could do what, given the local control state) plus the method-pack factors for threat strength and initiation. It is not a residual-risk score.

14 material threat scenario(s) in this issue.

Index	Threat	Component	Priority	Controls	Why
T21	Data interception / adversarial	Server (access hop)	high	C21 · 5.14 Information transfer · implemented	We do not know whether transport protection is in place for Server (access hop). If it is missing, an external attacker could read or alter data in transit. ISO mapping: 8.24 Use of cryptography; 5.14 Information transfer; 8.20 Network security. Threat strength medium strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.

Index	Threat	Component	Priority	Controls	Why
T22	Authentication attack / adversarial	Server (access hop)	high	C22 · 5.17 Authentication information · implemented	We do not know whether authentication is in place for Server (access hop). If it is missing, an external attacker could guess, steal, or bypass a login. ISO mapping: 8.5 Secure authentication; 5.17 Authentication information. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T23	Authorization attack / adversarial	Server (access hop)	high	C23 · 5.15 Access control · implemented	We do not know whether authorization is in place for Server (access hop). If it is missing, an external attacker could act with more access than they should have. ISO mapping: 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T26	Data disclosure / adversarial	Server (access hop)	high	C26 · 8.15 Logging · implemented	We do not know whether logging is in place for Server (access hop). If it is missing, an external attacker could go unnoticed after accessing data or systems. ISO mapping: 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T24	Authorization attack / adversarial	Server (access hop)	high	C24 · 8.22 Segregation of networks · implemented	We do not know whether boundary protection is in place for Server (access hop). If it is missing, an external attacker could cross a trust boundary they should not. ISO mapping: 8.22 Segregation of networks. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An

Index	Threat	Component	Priority	Controls	Why
					elevated public profile may raise strength one step. These are table lookups, not AI.
T27	Authorization attack / adversarial	Server	high	C27 · 5.15 Access control · implemented	We do not know whether authorization is in place for Server. If it is missing, an external attacker could act with more access than they should have. ISO mapping: 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T28	Data disclosure / adversarial	Server	high	C28 · 8.11 Data masking · implemented	We do not know whether data-at-rest protection is in place for Server. If it is missing, an external attacker could read stored data. ISO mapping: 8.24 Use of cryptography; 8.11 Data masking; 8.12 Data leakage prevention. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T30	Data disclosure / adversarial	Server	high	C30 · 8.15 Logging · implemented	We do not know whether logging is in place for Server. If it is missing, an external attacker could go unnoticed after accessing data or systems. ISO mapping: 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T29	Data modification / adversarial	Server	high	C29 · 8.26 Application security requirements · unknown	We do not know whether input validation is in place for Server. If it is missing, an external attacker could inject or alter submitted data. ISO mapping: 8.26 Application security requirements. Threat strength high strength is a method-pack lookup for this control type and weakness

Index	Threat	Component	Priority	Controls	Why
					(method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T31	Data modification / accidental	Server	medium	C31 · 8.25 Secure development life cycle · not implemented	We do not know whether secure operations and change is in place for Server. If it is missing, accidental misuse or error could change how the service is run, by mistake or misuse. ISO mapping: 8.4 Access to source code; 8.25 Secure development life cycle; 8.27 Secure system architecture and engineering principles; and 6 more. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T14	Social engineering / internal	Organisation	high	C14 · 5.1 Policies for information security · implemented	We do not know whether information security governance is in place for this organisation. If it is missing, someone inside the organisation could socially engineer staff or processes. ISO mapping: 5.1 Policies for information security; 5.2 Information security roles and responsibilities; 5.3 Segregation of duties; and 32 more. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (exposure unknown). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T15	Denial of service / environmental	Platform / delivery	high	C15 · 5.23 Information security for use of cloud services · not implemented	We do not know whether platform hardening is in place for the delivery platform. If it is missing, an environmental or infrastructure failure could disrupt the hosting or platform layer. ISO mapping: 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. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (exposure unknown). Likelihood of initiation unknown is source × exposure. An elevated public

Index	Threat	Component	Priority	Controls	Why
					profile may raise strength one step. These are table lookups, not AI.
T32	Data disclosure / adversarial	Server	high	C32 · 5.17 Authentication information · implemented	We do not know whether secrets protection is in place for Server. If it is missing, an external attacker could obtain keys or credentials. ISO mapping: 5.17 Authentication information. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T25	Data modification / adversarial	Server (access hop)	high	C25 · 8.26 Application security requirements · partially implemented	We do not know whether input validation is in place for Server (access hop). If it is missing, an external attacker could inject or alter submitted data. ISO mapping: 8.26 Application security requirements. Threat strength high strength is a method-pack lookup for this control type and weakness (method-pack mapping), then exposure (internal exposure). Likelihood of initiation unknown is source × exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.

5.2 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

Vendor	Component	Risk	Current residual	Decision
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
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 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	Security Engineer (organisation)	mitigate	remediation	Remediate input validation weakness; Allow-list validation and output encoding at the trust boundary; Edge filtering (WAF / API schema) in front of this input	M
Logging for Server → SQL is adequate protection. An external	Server → SQL	Security Engineer (organisation)	mitigate	remediation	Remediate logging weakness; Security-relevant logs shipped	M

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
attacker could go unnoticed after accessing data or systems. Current risk medium.					to SIEM with retention and alerting; Protected local security logs with time sync	
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
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	Server	Security Engineer	mitigate	remediation	Remediate secure operations and	M

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
protection. Accidental misuse or error could change how the service is run, by mistake or misuse. Current risk medium.		(organisation)			change weakness; Secure development and change-control programme; Malware protection and monitoring on operational components	
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 protection. An external attacker could guess, steal, or bypass a login. Current risk low.	Server → SQL	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
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

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
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 strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	Server (access hop)	Security Engineer (organisation)	accept	—	No treatment — accepted at P7.	S
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	Server	Security Engineer	accept	—	No treatment — accepted at P7.	S

Risk	Component	Responsible party	Decision	Treatment	Suggested remediation	Effort
external attacker could act with more access than they should have. Current risk low.		(organisation)				
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
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 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. Assumptions, Exceptions and Limitations

None recorded.

8. Conclusion

The assessed residual risk position for **Riskonami** is **high** and is **outside risk appetite** relative to the declared risk appetite. Outstanding management decisions, risk treatments and control actions are recorded above.

Appendix A — Control Posture

Control posture counts this organisation's controls only. Partner-owned controls are in Vendor responsibility, not mixed into these totals.

Relevant	Implemented	Partial	Not implemented	Unknown
85	59	1	24	1

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

Index	Control	What this control requires	Component	Who	Implementation	Related threats
C15	5.23 Information security for use of cloud services	Specify information-security requirements for the cloud service and manage them through acquisition, use and exit of that service.	Platform / delivery	organisation	not implemented	T15
C15	5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	Platform / delivery	organisation	not implemented	T15
C15	5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	Platform / delivery	organisation	not implemented	T15
C15	8.13 Information backup	Take copies of information, software and systems, and test restoration, according to an agreed backup policy.	Platform / delivery	organisation	not implemented	T15
C15	8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	Platform / delivery	organisation	not implemented	T15
C15	8.18 Use of privileged utility programs	Restrict and control use of utility programs that can override system and application controls.	Platform / delivery	organisation	not implemented	T15
C15	8.19 Installation of software on operational systems	Control installation of software on operational systems so only authorised, needed software is present.	Platform / delivery	organisation	not implemented	T15
C15	8.20 Network security	Secure networks, information systems and applications on those	Platform / delivery	organisation	not implemented	T15

Index	Control	What this control requires	Component	Who	Implementation	Related threats
		networks, including information in transit.				
C15	8.21 Security of network services	Identify, implement and monitor security mechanisms, service levels and requirements for network services.	Platform / delivery	organisation	not implemented	T15
C15	8.22 Segregation of networks	Segregate groups of information services, users and information systems on networks according to the access-control policy.	Platform / delivery	organisation	not implemented	T15
C15	8.23 Web filtering	Manage access to external websites to reduce exposure to malicious content.	Platform / delivery	organisation	not implemented	T15
C15	8.6 Capacity management	Monitor and adjust capacity so availability and performance requirements are met.	Platform / delivery	organisation	not implemented	T15
C15	8.7 Protection against malware	Protect against malware through detection, prevention and recovery measures, combined with user awareness.	Platform / delivery	organisation	not implemented	T15
C15	8.8 Management of technical vulnerabilities	Obtain information about technical vulnerabilities, evaluate exposure, and take timely action to address the risk.	Platform / delivery	organisation	not implemented	T15
C15	8.9 Configuration management	Define, implement, monitor and review security configurations of hardware, software, services and networks.	Platform / delivery	organisation	not implemented	T15
C31	8.25 Secure development life cycle	Establish and apply rules for the secure development of software and systems.	Server	organisation	not implemented	T31
C29	8.26 Application security requirements	Identify, specify and approve information-security requirements for applications, including those that support	Server	organisation	unknown	T29

Index	Control	What this control requires	Component	Who	Implementation	Related threats
		transactions and payments.				
C31	8.27 Secure system architecture and engineering principles	Specify and apply secure engineering principles to the design and implementation of information systems.	Server	organisation	not implemented	T31
C31	8.28 Secure coding	Apply secure coding principles to software development so common weaknesses are prevented.	Server	organisation	not implemented	T31
C31	8.29 Security testing in development and acceptance	Define and apply security testing processes in development and acceptance of information systems.	Server	organisation	not implemented	T31
C31	8.31 Separation of development, test and production environments	Separate development, test and production environments, and protect the production environment from those used for development and testing.	Server	organisation	not implemented	T31
C31	8.32 Change management	Control changes to information-processing facilities and systems through a documented change-management process.	Server	organisation	not implemented	T31
C31	8.33 Test information	Select, protect and manage test information so production data is not improperly used or exposed in test.	Server	organisation	not implemented	T31
C31	8.34 Protection of information systems during audit testing	Plan and control audit tests on operational systems so audit activity does not disrupt or weaken security.	Server	organisation	not implemented	T31
C31	8.4 Access to source code	Manage read and write access to source code, development tools and software libraries.	Server	organisation	not implemented	T31

Index	Control	What this control requires	Component	Who	Implementation	Related threats
C25	8.26 Application security requirements	Identify, specify and approve information-security requirements for applications, including those that support transactions and payments.	Server (access hop)	organisation	partially implemented	T25

Generated by Riskonami from assessment data version v2. Narrative enrichment, where enabled, does not replace the underlying deterministic risk, threat, control or treatment records.