



Engineering Risk Assessment Report

Assessment: Riskonami

System / Service: Riskonami

Assessment date: 2026-10-01

Assessment version: v2

Prepared for: Management and engineering

Technical owner: Musmato

Risk owner: Musmato

1. Technical Assessment

This assessment evaluates the technical risk of **Riskonami**. It covers the in-scope components listed in Section 2.2. The current residual risk is **high** against a declared risk appetite of **Company can tolerate low risk**. The assessed position is **outside risk appetite**. The assessment identified **14** material threat scenarios and **26** open control gaps requiring engineering or control-owner attention.

The principal technical risk drivers are **Input validation on Server; Logging on Server → SQL; Platform hardening on Platform / delivery**. The detailed threat, risk, control and remediation records below provide the traceable basis for remediation.

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 and Boundaries

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 Intended Audience

Management and engineering

2.4 Risk Appetite

Company can tolerate low risk

2.5 Assessment Method and Basis

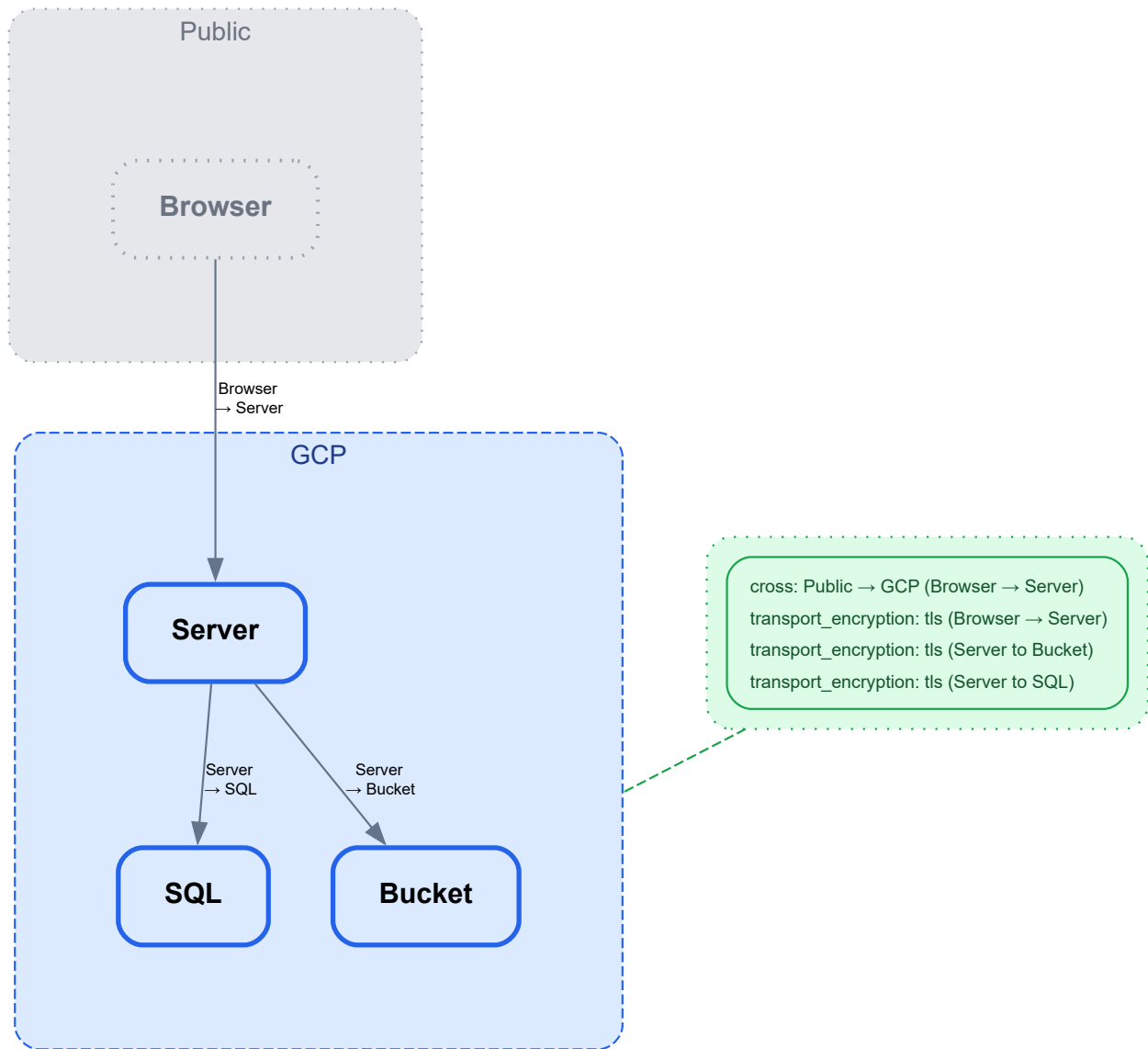
IRAM2 v2

3. System and Architecture Context

3.1 System Overview

ok this is a next.js application located in Google Cloud run

3.2 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)

3.3 Components and Services

Id	Name
app-ymerwyl9	Browser
app-zfpkopua	Server
app-7jihsriz	Bucket
app-br9qylo7	SQL

3.4 Data Flows, Interfaces and Trust Boundaries

Flow	Trust zones
Browser → Server	Public, GCP
Server to Bucket	Public, GCP
Server to SQL	Public, GCP

3.5 External Dependencies

Vendor	Zone	Responsibility
Google	GCP, Public	third_party
ISP	Public	third_party

4. Threat Model

4.1 Threat Posture Summary

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.

4.2 Material Threat Scenarios

Index	Threat	Component	Priority	Residual likelihood	Controls	Why
T21	Data interception / adversarial	Server (access hop)	high	low	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.
T22	Authentication attack / adversarial	Server (access hop)	high	low	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

Index	Threat	Component	Priority	Residual likelihood	Controls	Why
						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	low	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	medium	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 ×

Index	Threat	Component	Priority	Residual likelihood	Controls	Why
						exposure. An elevated public profile may raise strength one step. These are table lookups, not AI.
T24	Authorization attack / adversarial	Server (access hop)	high	medium	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 elevated public profile may raise strength one step. These are table lookups, not AI.
T27	Authorization attack / adversarial	Server	high	low	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	low	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

Index	Threat	Component	Priority	Residual likelihood	Controls	Why
						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	medium	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	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 (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	medium	C31 · 8.25 Secure development	We do not know whether secure operations and change is in place for Server. If it is missing,

Index	Threat	Component	Priority	Residual likelihood	Controls	Why
					life cycle · not implemented	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	low	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	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

Index	Threat	Component	Priority	Residual likelihood	Controls	Why
						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 profile may raise strength one step. These are table lookups, not AI.
T32	Data disclosure / adversarial	Server	high	medium	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	low	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. Risk Analysis

5.1 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.

5.2 Risk Register

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.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
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	remediation	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.	Remediate input validation weakness; Allow-list validation and output encoding at the trust boundary; Edge filtering (WAF / API schema) in front of this input
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	remediation	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	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
					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 layer. Current risk medium.	Platform / delivery	medium	mitigate	remediation	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.	Remediate platform hardening weakness; Secure configuration and hardening baseline; Vulnerability management and patch programme
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.	No treatment — accepted at P7.
Boundary protection for Server (access hop) is adequate protection. An external attacker	Server (access hop)	medium	accept	—	Negative -2 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown boundary	No treatment — accepted at P7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
could cross a trust boundary they should not. Current risk medium.					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	remediation	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.	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local security logs with time sync
Logging for Server is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	Server	medium	mitigate	remediation	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;	Remediate logging weakness; Security-relevant logs shipped to SIEM with retention and alerting; Protected local

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
					Protected local security logs with time sync Relevant ISO (not a cause): 8.15 Logging; 8.16 Monitoring activities; 8.17 Clock synchronization.	security logs with time sync
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	medium	mitigate	remediation	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.	Remediate secure operations and 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	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.	No treatment — accepted at P7.
Transport protection for Server → SQL is strong	Server → SQL	low	accept	—	Negative -1 CIA confidentiality high, integrity high, availability medium; medium	No treatment — accepted at P7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
protection. An external attacker could read or alter data in transit. Current risk low.					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;	No treatment — accepted at P7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
					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 Relevant ISO (not a cause): 5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; and 1 more.	No treatment — accepted at p7.
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.	No treatment — accepted at p7.
Transport protection for Server → Bucket is strong protection. An	Server → Bucket	low	accept	—	Negative -1 CIA confidentiality high, integrity high, availability medium; medium	No treatment — accepted at p7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
external attacker could read or alter data in transit. Current risk low.					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;	No treatment — accepted at P7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
					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	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.	No treatment — accepted at P7.
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.	No treatment — accepted at P7.
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:	No treatment — accepted at P7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
					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.	No treatment — accepted at P7.
Input validation for Server (access hop) is strong protection. An external attacker could inject or alter submitted	Server (access hop)	low	accept	—	Negative -1 CIA confidentiality high, integrity high, availability medium; high strength, initiation possible; unknown input validation state; not in place: Edge	No treatment — accepted at P7.

Risk	Component	Current residual	Decision	Treatment	Why	Suggested remediation
data. Current risk low.					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.	No treatment — accepted at P7.
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.	No treatment — accepted at P7.

6. Control Assessment

6.1 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

6.2 Detailed Control Assessment

Each row names the ISO control and **what this control requires**, so the assessment is readable without a separate catalogue.

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
C14	5.1 Policies for information security	Issue, approve, communicate and review information-security policies that set direction for the organisation.	Organisation	org	implemented	organisation	T14
C14	5.10 Acceptable use of information and other associated assets	Define and enforce acceptable use of information and associated assets by personnel and external parties.	Organisation	org	implemented	organisation	T14
C14	5.11 Return of assets	Recover organisation assets when employment, contracts or roles end.	Organisation	org	implemented	organisation	T14
C14	5.12 Classification of information	Classify information according to its value, legal obligations and business need so handling rules follow	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		that classification.					
C14	5.13 Labelling of information	Label information according to the classification scheme so handlers know how to treat it.	Organisation	org	implemented	organisation	T14
C14	5.16 Identity management	Manage identities through their lifecycle so people and systems can be uniquely identified and granted only the access they need.	Organisation	org	implemented	organisation	T14
C14	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.	Organisation	org	implemented	organisation	T14
C14	5.2 Information security roles and responsibilities	Define and assign information-security roles and responsibilities so it is clear who owns, operates and is accountable for each control.	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
C14	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.	Organisation	org	implemented	organisation	T14
C14	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.	Organisation	org	implemented	organisation	T14
C14	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.	Organisation	org	implemented	organisation	T14
C14	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.	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
C14	5.24 Information security incident management planning and preparation	Plan and prepare to detect, report, assess and respond to information-security incidents in a consistent way.	Organisation	org	implemented	organisation	T14
C14	5.25 Assessment and decision on information security events	Assess information-security events and decide which are incidents that require a response.	Organisation	org	implemented	organisation	T14
C14	5.26 Response to information security incidents	Respond to information-security incidents according to documented procedures.	Organisation	org	implemented	organisation	T14
C14	5.27 Learning from information security incidents	Capture lessons from incidents and use them to improve controls and procedures.	Organisation	org	implemented	organisation	T14
C14	5.28 Collection of evidence	Identify, collect, acquire and preserve evidence related to information-security events for investigations or legal use.	Organisation	org	implemented	organisation	T14
C14	5.3 Segregation of duties	Separate conflicting duties and areas of responsibility so one person	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		cannot both commit and conceal a security failure or fraud.					
C14	5.31 Legal, statutory, regulatory and contractual requirements	Identify and meet legal, statutory, regulatory and contractual information-security requirements.	Organisation	org	implemented	organisation	T14
C14	5.32 Intellectual property rights	Protect intellectual property and use software and other IP in accordance with licence and law.	Organisation	org	implemented	organisation	T14
C14	5.33 Protection of records	Protect records from loss, destruction, falsification and unauthorised access or release, according to requirements.	Organisation	org	implemented	organisation	T14
C14	5.34 Privacy and protection of PII	Protect personally identifiable information in accordance with applicable privacy law and the organisation's privacy commitments.	Organisation	org	implemented	organisation	T14
C14	5.35 Independent review of information security	Independently review the organisation's approach to managing	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		information security at planned intervals and when significant changes occur.					
C14	5.36 Compliance with policies, rules and standards for information security	Regularly review compliance with information-security policies, rules and standards.	Organisation	org	implemented	organisation	T14
C14	5.37 Documented operating procedures	Document and maintain operating procedures for information-processing activities.	Organisation	org	implemented	organisation	T14
C14	5.4 Management responsibilities	Require management to require personnel to apply information security according to established policies and procedures.	Organisation	org	implemented	organisation	T14
C14	5.5 Contact with authorities	Identify authorities to contact for legal, regulatory and incident matters, and maintain those contacts.	Organisation	org	implemented	organisation	T14
C14	5.6 Contact with special interest groups	Maintain contact with specialist security groups	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		and professional forums that improve awareness of threats and good practice.					
C14	5.7 Threat intelligence	Collect and analyse threat information and use it to adjust protections, detections and response.	Organisation	org	implemented	organisation	T14
C14	5.8 Information security in project management	Include information security in project planning and delivery, not only after go-live.	Organisation	org	implemented	organisation	T14
C14	5.9 Inventory of information and other associated assets	Inventory information and associated assets, including owners, so they can be protected and accounted for.	Organisation	org	implemented	organisation	T14
C14	8.1 User endpoint devices	Protect information on user endpoint devices and restrict how those devices use, store and transfer it.	Organisation	org	implemented	organisation	T14
C14	8.10 Information deletion	Delete information in information systems, devices or storage media	Organisation	org	implemented	organisation	T14

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		when it is no longer required, using a method that prevents recovery.					
C14	8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that do not need the real values cannot see them.	Organisation	org	implemented	organisation	T14
C14	8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	Organisation	org	implemented	organisation	T14
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	org	not implemented	organisation	T15
C15	5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	Platform / delivery	org	not implemented	organisation	T15
C15	5.30 ICT readiness for	Plan ICT so information-	Platform / delivery	org	not implemented	organisation	T15

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
	business continuity	processing can continue, recover and meet availability objectives during disruption.					
C15	8.13 Information backup	Take copies of information, software and systems, and test restoration, according to an agreed backup policy.	Platform / delivery	org	not implemented	organisation	T15
C15	8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	Platform / delivery	org	not implemented	organisation	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	org	not implemented	organisation	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	org	not implemented	organisation	T15
C15	8.20 Network security	Secure networks, information systems and applications on	Platform / delivery	org	not implemented	organisation	T15

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		those 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	org	not implemented	organisation	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	org	not implemented	organisation	T15
C15	8.23 Web filtering	Manage access to external websites to reduce exposure to malicious content.	Platform / delivery	org	not implemented	organisation	T15
C15	8.6 Capacity management	Monitor and adjust capacity so availability and performance requirements are met.	Platform / delivery	org	not implemented	organisation	T15
C15	8.7 Protection against malware	Protect against malware through detection, prevention and recovery measures,	Platform / delivery	org	not implemented	organisation	T15

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		combined with user awareness.					
C15	8.8 Management of technical vulnerabilities	Obtain information about technical vulnerabilities, evaluate exposure, and take timely action to address the risk.	Platform / delivery	org	not implemented	organisation	T15
C15	8.9 Configuration management	Define, implement, monitor and review security configurations of hardware, software, services and networks.	Platform / delivery	org	not implemented	organisation	T15
C27	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server	org	implemented	organisation	T27
C32	5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server	org	implemented	organisation	T32
C27	5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server	org	implemented	organisation	T27

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
C28	8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that do not need the real values cannot see them.	Server	org	implemented	organisation	T28
C28	8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	Server	org	implemented	organisation	T28
C30	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server	org	implemented	organisation	T30
C30	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server	org	implemented	organisation	T30
C30	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so	Server	org	implemented	organisation	T30

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		events can be correlated.					
C27	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server	org	implemented	organisation	T27
C28	8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of the information.	Server	org	implemented	organisation	T28
C31	8.25 Secure development life cycle	Establish and apply rules for the secure development of software and systems.	Server	org	not implemented	organisation	T31
C29	8.26 Application security requirements	Identify, specify and approve information-security requirements for applications, including those that support transactions and payments.	Server	org	unknown	organisation	T29
C31	8.27 Secure system architecture and engineering principles	Specify and apply secure engineering principles to the design and implementation of information systems.	Server	org	not implemented	organisation	T31
C31	8.28 Secure coding	Apply secure coding principles to	Server	org	not implemented	organisation	T31

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		software development so common weaknesses are prevented.					
C31	8.29 Security testing in development and acceptance	Define and apply security testing processes in development and acceptance of information systems.	Server	org	not implemented	organisation	T31
C27	8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server	org	implemented	organisation	T27
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	org	not implemented	organisation	T31
C31	8.32 Change management	Control changes to information-processing facilities and systems through a documented change-management process.	Server	org	not implemented	organisation	T31
C31	8.33 Test information	Select, protect and manage	Server	org	not implemented	organisation	T31

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		test information so production data is not improperly used or exposed in test.					
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	org	not implemented	organisation	T31
C31	8.4 Access to source code	Manage read and write access to source code, development tools and software libraries.	Server	org	not implemented	organisation	T31
C21	5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server (access hop)	org	implemented	organisation	T21
C23	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server (access hop)	org	implemented	organisation	T23
C22	5.17 Authentication information	Allocate, protect and change authentication secrets	Server (access hop)	org	implemented	organisation	T22

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		(passwords, keys, tokens) throughout their life.					
C23	5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server (access hop)	org	implemented	organisation	T23
C26	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server (access hop)	org	implemented	organisation	T26
C26	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server (access hop)	org	implemented	organisation	T26
C26	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server (access hop)	org	implemented	organisation	T26
C23	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server (access hop)	org	implemented	organisation	T23

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
C21	8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server (access hop)	org	implemented	organisation	T21
C24	8.22 Segregation of networks	Segregate groups of information services, users and information systems on networks according to the access-control policy.	Server (access hop)	org	implemented	organisation	T24
C21	8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of the information.	Server (access hop)	org	implemented	organisation	T21
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)	org	partially implemented	organisation	T25
C23	8.3 Information access restriction	Restrict access to information and other associated assets	Server (access hop)	org	implemented	organisation	T23

Index	Control	What this control requires	Component	Disposition	Implementation	Who	Related threats
		according to the access-control policy.					
C22	8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server (access hop)	org	implemented	organisation	T22

6.3 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

7. Engineering Remediation Plan

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

8. Residual Risk

Risk	Current residual
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.	high
Logging for Server → SQL is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	medium
Platform hardening for the delivery platform is no protection. An environmental or infrastructure failure could disrupt the hosting or platform layer. Current risk medium.	medium
Logging for Server → Bucket is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	medium
Boundary protection for Server (access hop) is adequate protection. An external attacker could cross a trust boundary they should not. Current risk medium.	medium
Logging for Server (access hop) is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	medium
Logging for Server is adequate protection. An external attacker could go unnoticed after accessing data or systems. Current risk medium.	medium
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.	medium
Secrets protection for Server is adequate protection. An external attacker could obtain keys or credentials. Current risk medium.	medium
Transport protection for Server → SQL is strong protection. An external attacker could read or alter data in transit. Current risk low.	low
Authentication for Server → SQL is strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	low
Authorization for Server → SQL is strong protection. An external attacker could act with more access than they should have. Current risk low.	low
Information security governance for this organisation is strong protection. Someone inside the organisation could socially engineer staff or processes. Current risk low.	low
Transport protection for Server → Bucket is strong protection. An external attacker could read or alter data in transit. Current risk low.	low
Authentication for Server → Bucket is strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	low
Authorization for Server → Bucket is strong protection. An external attacker could act with more access than they should have. Current risk low.	low
Transport protection for Server (access hop) is strong protection. An external attacker could read or alter data in transit. Current risk low.	low
Authentication for Server (access hop) is strong protection. An external attacker could guess, steal, or bypass a login. Current risk low.	low
Authorization for Server (access hop) is strong protection. An external attacker could act with more access than they should have. Current risk low.	low
Input validation for Server (access hop) is strong protection. An external attacker could inject or alter submitted data. Current risk low.	low

Risk	Current residual
Authorization for Server is strong protection. An external attacker could act with more access than they should have. Current risk low.	low
Data-at-rest protection for Server is strong protection. An external attacker could read stored data. Current risk low.	low

9. Exceptions, Assumptions and Uncertainty

None recorded.

10. Traceability

None recorded.

Generated by Riskonami from assessment data version v2. All detailed risks, controls, owners, evidence states and remediation actions are generated deterministically from the assessment record. Narrative enrichment, where enabled, only explains that data.