



Overall Compliance Report

Assessment: Riskonami

System / Service: Riskonami

Assessment date: 2026-10-01

Assessment version: v2

Control register owner: Musmato

Risk owner: Musmato

1. Compliance Statement

This register combines organisational in-place state with **accepted** vendor compliance answers for **Riskonami**. It contains **140** combined controls, of which **114** are implemented, **1** are partially implemented, **24** are not implemented and **1** remain unresolved. Submitted but unaccepted vendor answers stay UNKNOWN.

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).

3. Threats

The register cites these threats by key. Each key is listed here with the threat it names.

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.

Index	Threat	Component	Priority	Why
T1	Supply-chain attack / supplier	Bucket	high	We do not know whether supplier assurance is in place for Bucket. If it is missing, a supplier or third party could abuse a supplier or third-party path into this system. ISO mapping: 5.19 Information security in supplier

Index	Threat	Component	Priority	Why
				relationships; 5.20 Addressing information security within supplier agreements; 5.21 Managing information security in the ICT supply chain; 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.
T2	Data disclosure / adversarial	Bucket	high	We do not know whether logging is in place for Bucket. 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.
T3	Denial of service / adversarial	Bucket	high	We do not know whether backup and restore is in place for Bucket. If it is missing, an external attacker could interrupt or degrade the service. ISO mapping: 8.13 Information backup; 8.14 Redundancy of information processing facilities; 5.29 Information security during disruption; 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.
T4	Data interception / adversarial	Server → SQL	high	We do not know whether transport protection is in place for Server → SQL. 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.
T5	Authentication attack / adversarial	Server → SQL	high	We do not know whether authentication is in place for Server → SQL. 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.
T6	Authorization attack / adversarial	Server → SQL	high	We do not know whether authorization is in place for Server → SQL. 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.
T7	Data disclosure / adversarial	Server → SQL	high	We do not know whether logging is in place for Server → SQL. 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.

Index	Threat	Component	Priority	Why
				An elevated public profile may raise strength one step. These are table lookups, not AI.
T8	Authentication attack / adversarial	SQL	high	We do not know whether authentication is in place for SQL. 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.
T9	Authorization attack / adversarial	SQL	high	We do not know whether authorization is in place for SQL. 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.
T10	Data disclosure / adversarial	SQL	high	We do not know whether data-at-rest protection is in place for SQL. 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.
T11	Data disclosure / adversarial	SQL	high	We do not know whether logging is in place for SQL. 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.
T12	Denial of service / adversarial	SQL	high	We do not know whether backup and restore is in place for SQL. If it is missing, an external attacker could interrupt or degrade the service. ISO mapping: 8.13 Information backup; 8.14 Redundancy of information processing facilities; 5.29 Information security during disruption; 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.
T13	Supply-chain attack / supplier	SQL	high	We do not know whether supplier assurance is in place for SQL. If it is missing, a supplier or third party could abuse a supplier or third-party path into this system. ISO mapping: 5.19 Information security in supplier relationships; 5.20 Addressing information security within supplier agreements; 5.21 Managing information security in the ICT supply chain; and 1 more. 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 /	Organisation	high	We do not know whether information security governance is in place for this organisation. If it is missing, someone inside the organisation could socially

Index	Threat	Component	Priority	Why
	internal			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	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 profile may raise strength one step. These are table lookups, not AI.
T16	Supply-chain attack / supplier	GCP	high	We do not know whether supplier assurance is in place for GCP. If it is missing, a supplier or third party could abuse a supplier or third-party path into this system. ISO mapping: 5.19 Information security in supplier relationships; 5.20 Addressing information security within supplier agreements; 5.21 Managing information security in the ICT supply chain; and 1 more. 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.
T17	Data interception / adversarial	Server → Bucket	high	We do not know whether transport protection is in place for Server → Bucket. 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.
T18	Authentication attack / adversarial	Server → Bucket	high	We do not know whether authentication is in place for Server → Bucket. 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.
T19	Authorization attack / adversarial	Server → Bucket	high	We do not know whether authorization is in place for Server → Bucket. 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.
T20	Data disclosure / adversarial	Server → Bucket	high	We do not know whether logging is in place for Server → Bucket. 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

Index	Threat	Component	Priority	Why
				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.
T21	Data interception / adversarial	Server (access hop)	high	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	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	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.
T24	Authorization attack / adversarial	Server (access hop)	high	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.
T25	Data modification / adversarial	Server (access hop)	high	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.
T26	Data disclosure / adversarial	Server (access hop)	high	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.
T27	Authorization attack / adversarial	Server	high	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

Index	Threat	Component	Priority	Why
				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	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.
T29	Data modification / adversarial	Server	high	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.
T30	Data disclosure / adversarial	Server	high	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.
T31	Data modification / accidental	Server	medium	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.
T32	Data disclosure / adversarial	Server	high	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.

4. Combined Control Register

Each row names the ISO control and **what this control requires**. **Component count** is how many places that control appears in this register.

Owner is who holds the control on that component: a named party in this organisation, or the vendor. Vendor-held controls are in this register under the vendor's name, and summarised under Vendor responsibility. The same ISO control on more than one component is an instance copy, not a second catalogue topic.

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C1	5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	Bucket	4	unknown	Google	Establish contractual security requirements with third party	T1
C1	5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	Bucket	4	unknown	Google	Establish contractual security requirements with third party	T1
C1	5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	Bucket	4	unknown	Google	Establish contractual security requirements with third party	T1
C1	5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	Bucket	4	unknown	Google	Establish contractual security requirements with third party	T1
C3	5.29 Information security during disruption	Maintain information security at an agreed level	Bucket	3	unknown	Google	Establish contractual security requirements	T3

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		during disruption.					with third party	
C3	5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	Bucket	3	unknown	Google	Establish contractual security requirements with third party	T3
C3	8.13 Information backup	Take copies of information, software and systems, and test restoration, according to an agreed backup policy.	Bucket	3	unknown	Google	Establish contractual security requirements with third party	T3
C3	8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	Bucket	3	unknown	Google	Establish contractual security requirements with third party	T3
C2	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Bucket	6	unknown	Google	Establish contractual security requirements with third party	T2
C2	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Bucket	6	unknown	Google	Establish contractual security requirements with third party	T2
C2	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a	Bucket	6	unknown	Google	Establish contractual security requirements	T2

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		trusted time source so events can be correlated.					with third party	
C16	5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	GCP	4	unknown	Google	Establish contractual security requirements with third party	T16
C16	5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	GCP	4	unknown	Google	Establish contractual security requirements with third party	T16
C16	5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	GCP	4	unknown	Google	Establish contractual security requirements with third party	T16
C16	5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	GCP	4	unknown	Google	Establish contractual security requirements with third party	T16

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C14	5.1 Policies for information security	Issue, approve, communicate and review information-security policies that set direction for the organisation.	Organisation	1	implemented	Musmato	—	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	1	implemented	Musmato	—	T14
C14	5.11 Return of assets	Recover organisation assets when employment, contracts or roles end.	Organisation	1	implemented	Musmato	—	T14
C14	5.12 Classification of information	Classify information according to its value, legal obligations and business need so handling rules follow that classification.	Organisation	1	implemented	Musmato	—	T14
C14	5.13 Labelling of information	Label information according to the classification scheme so handlers know how to treat it.	Organisation	1	implemented	Musmato	—	T14
C14	5.16 Identity management	Manage identities through their lifecycle so people and systems can be uniquely identified and granted only	Organisation	1	implemented	Musmato	—	T14

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		the access they need.						
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	4	implemented	Musmato	—	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	1	implemented	Musmato	—	T14
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	4	implemented	Musmato	—	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	4	implemented	Musmato	—	T14
C14	5.22 Monitoring,	Monitor and review the	Organisation	4	implemented	Musmato	—	T14

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
	review and change management of supplier services	supplier's service against the agreed security requirements, and manage changes so security is not weakened.						
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	2	implemented	Musmato	—	T14
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	1	implemented	Musmato	—	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	1	implemented	Musmato	—	T14
C14	5.26 Response to information security incidents	Respond to information-security incidents according to documented procedures.	Organisation	1	implemented	Musmato	—	T14
C14	5.27 Learning from information security incidents	Capture lessons from incidents and use them to improve controls and procedures.	Organisation	1	implemented	Musmato	—	T14

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C14	5.28 Collection of evidence	Identify, collect, acquire and preserve evidence related to information-security events for investigations or legal use.	Organisation	1	implemented	Musmato	—	T14
C14	5.3 Segregation of duties	Separate conflicting duties and areas of responsibility so one person cannot both commit and conceal a security failure or fraud.	Organisation	1	implemented	Musmato	—	T14
C14	5.31 Legal, statutory, regulatory and contractual requirements	Identify and meet legal, statutory, regulatory and contractual information-security requirements.	Organisation	1	implemented	Musmato	—	T14
C14	5.32 Intellectual property rights	Protect intellectual property and use software and other IP in accordance with licence and law.	Organisation	1	implemented	Musmato	—	T14
C14	5.33 Protection of records	Protect records from loss, destruction, falsification and unauthorised access or release, according to requirements.	Organisation	1	implemented	Musmato	—	T14
C14	5.34 Privacy and protection of PII	Protect personally identifiable information in accordance	Organisation	1	implemented	Musmato	—	T14

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		with applicable privacy law and the organisation's privacy commitments.						
C14	5.35 Independent review of information security	Independently review the organisation's approach to managing information security at planned intervals and when significant changes occur.	Organisation	1	implemented	Musmato	—	T14
C14	5.36 Compliance with policies, rules and standards for information security	Regularly review compliance with information-security policies, rules and standards.	Organisation	1	implemented	Musmato	—	T14
C14	5.37 Documented operating procedures	Document and maintain operating procedures for information-processing activities.	Organisation	1	implemented	Musmato	—	T14
C14	5.4 Management responsibilities	Require management to require personnel to apply information security according to established policies and procedures.	Organisation	1	implemented	Musmato	—	T14
C14	5.5 Contact with authorities	Identify authorities to contact for legal, regulatory and incident matters, and	Organisation	1	implemented	Musmato	—	T14

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		maintain those contacts.						
C14	5.6 Contact with special interest groups	Maintain contact with specialist security groups and professional forums that improve awareness of threats and good practice.	Organisation	1	implemented	Musmato	—	T14
C14	5.7 Threat intelligence	Collect and analyse threat information and use it to adjust protections, detections and response.	Organisation	1	implemented	Musmato	—	T14
C14	5.8 Information security in project management	Include information security in project planning and delivery, not only after go-live.	Organisation	1	implemented	Musmato	—	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	1	implemented	Musmato	—	T14
C14	8.1 User endpoint devices	Protect information on user endpoint devices and restrict how those devices use, store and transfer it.	Organisation	1	implemented	Musmato	—	T14
C14	8.10 Information deletion	Delete information in information systems, devices or	Organisation	1	implemented	Musmato	—	T14

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		storage media 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	3	implemented	Musmato	—	T14
C14	8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	Organisation	3	implemented	Musmato	—	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	2	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	Platform / delivery	3	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability	Platform / delivery	3	not implemented	Musmato	Remediate platform hardening weakness	T15

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		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	3	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	Platform / delivery	3	not implemented	Musmato	Remediate platform hardening weakness	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	1	not implemented	Musmato	Remediate platform hardening weakness	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	1	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Platform / delivery	4	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.21 Security of network services	Identify, implement and monitor security mechanisms, service levels	Platform / delivery	1	not implemented	Musmato	Remediate platform hardening weakness	T15

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		and requirements for network services.						
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	2	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.23 Web filtering	Manage access to external websites to reduce exposure to malicious content.	Platform / delivery	1	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.6 Capacity management	Monitor and adjust capacity so availability and performance requirements are met.	Platform / delivery	1	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.7 Protection against malware	Protect against malware through detection, prevention and recovery measures, combined with user awareness.	Platform / delivery	1	not implemented	Musmato	Remediate platform hardening weakness	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	1	not implemented	Musmato	Remediate platform hardening weakness	T15
C15	8.9 Configuration management	Define, implement, monitor and	Platform / delivery	1	not implemented	Musmato	Remediate platform	T15

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		review security configurations of hardware, software, services and networks.					hardening weakness	
C27	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server	5	implemented	Musmato	—	T27
C32	5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server	5	implemented	Musmato	—	T32
C27	5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server	5	implemented	Musmato	—	T27
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	3	implemented	Musmato	—	T28

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C28	8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	Server	3	implemented	Musmato	—	T28
C30	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server	6	implemented	Musmato	Remediate logging weakness	T30
C30	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server	6	implemented	Musmato	Remediate logging weakness	T30
C30	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server	6	implemented	Musmato	Remediate logging weakness	T30
C27	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server	5	implemented	Musmato	—	T27
C28	8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of	Server	5	implemented	Musmato	—	T28

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		the information.						
C31	8.25 Secure development life cycle	Establish and apply rules for the secure development of software and systems.	Server	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C29	8.26 Application security requirements	Identify, specify and approve information-security requirements for applications, including those that support transactions and payments.	Server	2	unknown	Musmato	Remediate input validation weakness	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	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C31	8.28 Secure coding	Apply secure coding principles to software development so common weaknesses are prevented.	Server	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C31	8.29 Security testing in development and acceptance	Define and apply security testing processes in development and acceptance of information systems.	Server	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C27	8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server	5	implemented	Musmato	—	T27

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
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	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C31	8.32 Change management	Control changes to information-processing facilities and systems through a documented change-management process.	Server	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C31	8.33 Test information	Select, protect and manage test information so production data is not improperly used or exposed in test.	Server	1	not implemented	Musmato	Remediate secure operations and change weakness	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	1	not implemented	Musmato	Remediate secure operations and change weakness	T31
C31	8.4 Access to source code	Manage read and write access to source code, development tools and software libraries.	Server	1	not implemented	Musmato	Remediate secure operations and change weakness	T31

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C21	5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server (access hop)	3	implemented	Musmato	—	T21
C23	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server (access hop)	5	implemented	Musmato	—	T23
C22	5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server (access hop)	5	implemented	Musmato	—	T22
C23	5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server (access hop)	5	implemented	Musmato	—	T23
C26	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server (access hop)	6	implemented	Musmato	Remediate logging weakness	T26
C26	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server (access hop)	6	implemented	Musmato	Remediate logging weakness	T26

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C26	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server (access hop)	6	implemented	Musmato	Remediate logging weakness	T26
C23	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server (access hop)	5	implemented	Musmato	—	T23
C21	8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server (access hop)	4	implemented	Musmato	—	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)	2	implemented	Musmato	—	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)	5	implemented	Musmato	—	T21
C25	8.26 Application security requirements	Identify, specify and approve information-security requirements for	Server (access hop)	2	partially implemented	Musmato	—	T25

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		applications, including those that support transactions and payments.						
C23	8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server (access hop)	5	implemented	Musmato	—	T23
C22	8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server (access hop)	4	implemented	Musmato	—	T22
C17	5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server → Bucket	3	implemented	Musmato	—	T17
C19	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server → Bucket	5	implemented	Musmato	—	T19
C18	5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server → Bucket	5	implemented	Musmato	—	T18
C19	5.18 Access rights	Provision, review and revoke access rights according to	Server → Bucket	5	implemented	Musmato	—	T19

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		policy and when roles change.						
C20	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server → Bucket	6	implemented	Musmato	—	T20
C20	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server → Bucket	6	implemented	Musmato	—	T20
C20	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server → Bucket	6	implemented	Musmato	—	T20
C19	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server → Bucket	5	implemented	Musmato	—	T19
C17	8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server → Bucket	4	implemented	Musmato	—	T17
C17	8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the	Server → Bucket	5	implemented	Musmato	—	T17

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		classification of the information.						
C19	8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server → Bucket	5	implemented	Musmato	—	T19
C18	8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server → Bucket	4	implemented	Musmato	—	T18
C4	5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server → SQL	3	implemented	Musmato	—	T4
C6	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server → SQL	5	implemented	Musmato	—	T6
C5	5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server → SQL	5	implemented	Musmato	—	T5
C6	5.18 Access rights	Provision, review and revoke access rights according to policy and	Server → SQL	5	implemented	Musmato	—	T6

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		when roles change.						
C7	8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server → SQL	6	implemented	Musmato	Remediate logging weakness	T7
C7	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server → SQL	6	implemented	Musmato	Remediate logging weakness	T7
C7	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server → SQL	6	implemented	Musmato	Remediate logging weakness	T7
C6	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server → SQL	5	implemented	Musmato	—	T6
C4	8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server → SQL	4	implemented	Musmato	—	T4
C4	8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of	Server → SQL	5	implemented	Musmato	—	T4

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		the information.						
C6	8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server → SQL	5	implemented	Musmato	—	T6
C5	8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server → SQL	4	implemented	Musmato	—	T5
C9	5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	SQL	5	unknown	Google	Establish contractual security requirements with third party	T9
C8	5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	SQL	5	unknown	Google	Establish contractual security requirements with third party	T8
C9	5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	SQL	5	unknown	Google	Establish contractual security requirements with third party	T9
C13	5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the	SQL	4	unknown	Google	Establish contractual security requirements with third party	T13

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		customer information and assets the supplier can access or affect.						
C13	5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	SQL	4	unknown	Google	Establish contractual security requirements with third party	T13
C13	5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	SQL	4	unknown	Google	Establish contractual security requirements with third party	T13
C13	5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	SQL	4	unknown	Google	Establish contractual security requirements with third party	T13
C12	5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	SQL	3	unknown	Google	Establish contractual security requirements with third party	T12

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
C12	5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	SQL	3	unknown	Google	Establish contractual security requirements with third party	T12
C10	8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that do not need the real values cannot see them.	SQL	3	unknown	Google	Establish contractual security requirements with third party	T10
C10	8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	SQL	3	unknown	Google	Establish contractual security requirements with third party	T10
C12	8.13 Information backup	Take copies of information, software and systems, and test restoration, according to an agreed backup policy.	SQL	3	unknown	Google	Establish contractual security requirements with third party	T12
C12	8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	SQL	3	unknown	Google	Establish contractual security requirements with third party	T12
C11	8.15 Logging	Produce, protect, retain and review logs	SQL	6	unknown	Google	Establish contractual security	T11

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		of events that can support monitoring, investigation and evidence.					requirements with third party	
C11	8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	SQL	6	unknown	Google	Establish contractual security requirements with third party	T11
C11	8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	SQL	6	unknown	Google	Establish contractual security requirements with third party	T11
C9	8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	SQL	5	unknown	Google	Establish contractual security requirements with third party	T9
C10	8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of the information.	SQL	5	unknown	Google	Establish contractual security requirements with third party	T10
C9	8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	SQL	5	unknown	Google	Establish contractual security requirements with third party	T9
C8	8.5 Secure authentication	Authenticate users and systems with a mechanism	SQL	4	unknown	Google	Establish contractual security requirements	T8

Index	Control	What this control requires	Component	Component count	Implementation	Owner	Actions	Related threats
		whose strength matches the access being granted.					with third party	

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	Bucket	supplier	implemented	Vendor review — Google	We ensure all supplier relationships have security sections	ISO 27001 certification
5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	Bucket	supplier	implemented	Vendor review — Google	We ensure all supplier relationships have security sections	ISO 27001 certification
5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	Bucket	supplier	implemented	Vendor review — Google	We ensure all supplier relationships have security sections	ISO 27001 certification
5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	Bucket	supplier	implemented	Vendor review — Google	We ensure all supplier relationships have security sections	ISO 27001 certification

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
8.13 Information backup	Take copies of information, software and systems, and test restoration, according to an agreed backup policy.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Bucket	supplier	implemented	Vendor review — Google	—	ISO 27001 certification

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
5.19 Information security in supplier relationships	Agree and document the information-security requirements for this supplier relationship, covering the customer information and assets the supplier can access or affect.	GCP	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
5.20 Addressing information security within supplier agreements	Put those security requirements, responsibilities and assurance expectations into the supplier agreement or an equivalent binding instrument.	GCP	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
5.21 Managing information security in the ICT supply chain	Identify and manage information-security risk in the ICT supply chain for this service, including sub-suppliers and components the supplier relies on.	GCP	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
5.22 Monitoring, review and change management of supplier services	Monitor and review the supplier's service against the agreed security requirements, and manage changes so security is not weakened.	GCP	supplier	implemented	Vendor review — Google	—	ISO 27001 certification
5.1 Policies for information security	Issue, approve, communicate and review information-security policies that set direction for the organisation.	Organisation	org	implemented	This organisation	—	—
5.10 Acceptable use of	Define and enforce	Organisation	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
information and other associated assets	acceptable use of information and associated assets by personnel and external parties.						
5.11 Return of assets	Recover organisation assets when employment, contracts or roles end.	Organisation	org	implemented	This organisation	—	—
5.12 Classification of information	Classify information according to its value, legal obligations and business need so handling rules follow that classification.	Organisation	org	implemented	This organisation	—	—
5.13 Labelling of information	Label information according to the classification scheme so handlers know how to treat it.	Organisation	org	implemented	This organisation	—	—
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	This organisation	—	—
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	This organisation	—	—
5.2 Information security roles and responsibilities	Define and assign information-security roles and responsibilities so it is clear who	Organisation	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	owns, operates and is accountable for each control.						
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	This organisation	—	—
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	This organisation	—	—
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	This organisation	—	—
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	This organisation	—	—
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	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
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	This organisation	—	—
5.26 Response to information security incidents	Respond to information-security incidents according to documented procedures.	Organisation	org	implemented	This organisation	—	—
5.27 Learning from information security incidents	Capture lessons from incidents and use them to improve controls and procedures.	Organisation	org	implemented	This organisation	—	—
5.28 Collection of evidence	Identify, collect, acquire and preserve evidence related to information-security events for investigations or legal use.	Organisation	org	implemented	This organisation	—	—
5.3 Segregation of duties	Separate conflicting duties and areas of responsibility so one person cannot both commit and conceal a security failure or fraud.	Organisation	org	implemented	This organisation	—	—
5.31 Legal, statutory, regulatory and contractual requirements	Identify and meet legal, statutory, regulatory and contractual information-security requirements.	Organisation	org	implemented	This organisation	—	—
5.32 Intellectual property rights	Protect intellectual property and use software and other IP in accordance with licence and law.	Organisation	org	implemented	This organisation	—	—
5.33 Protection of records	Protect records from loss, destruction,	Organisation	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	falsification and unauthorised access or release, according to requirements.						
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	This organisation	—	—
5.35 Independent review of information security	Independently review the organisation's approach to managing information security at planned intervals and when significant changes occur.	Organisation	org	implemented	This organisation	—	—
5.36 Compliance with policies, rules and standards for information security	Regularly review compliance with information-security policies, rules and standards.	Organisation	org	implemented	This organisation	—	—
5.37 Documented operating procedures	Document and maintain operating procedures for information-processing activities.	Organisation	org	implemented	This organisation	—	—
5.4 Management responsibilities	Require management to require personnel to apply information security according to established policies and procedures.	Organisation	org	implemented	This organisation	—	—
5.5 Contact with authorities	Identify authorities to contact for legal, regulatory and incident matters,	Organisation	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	and maintain those contacts.						
5.6 Contact with special interest groups	Maintain contact with specialist security groups and professional forums that improve awareness of threats and good practice.	Organisation	org	implemented	This organisation	—	—
5.7 Threat intelligence	Collect and analyse threat information and use it to adjust protections, detections and response.	Organisation	org	implemented	This organisation	—	—
5.8 Information security in project management	Include information security in project planning and delivery, not only after go-live.	Organisation	org	implemented	This organisation	—	—
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	This organisation	—	—
8.1 User endpoint devices	Protect information on user endpoint devices and restrict how those devices use, store and transfer it.	Organisation	org	implemented	This organisation	—	—
8.10 Information deletion	Delete information in information systems, devices or storage media when it is no longer required, using a method that prevents recovery.	Organisation	org	implemented	This organisation	—	—
8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that	Organisation	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	do not need the real values cannot see them.						
8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	Organisation	org	implemented	This organisation	—	—
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	This organisation	—	—
5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	Platform / delivery	org	not implemented	This organisation	—	—
5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	Platform / delivery	org	not implemented	This organisation	—	—
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	This organisation	—	—
8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet	Platform / delivery	org	not implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	availability requirements.						
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	This organisation	—	—
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	This organisation	—	—
8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Platform / delivery	org	not implemented	This organisation	—	—
8.21 Security of network services	Identify, implement and monitor security mechanisms, service levels and requirements for network services.	Platform / delivery	org	not implemented	This organisation	—	—
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	This organisation	—	—
8.23 Web filtering	Manage access to external websites to reduce exposure to malicious content.	Platform / delivery	org	not implemented	This organisation	—	—
8.6 Capacity management	Monitor and adjust capacity so availability and performance requirements are met.	Platform / delivery	org	not implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
8.7 Protection against malware	Protect against malware through detection, prevention and recovery measures, combined with user awareness.	Platform / delivery	org	not implemented	This organisation	—	—
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	This organisation	—	—
8.9 Configuration management	Define, implement, monitor and review security configurations of hardware, software, services and networks.	Platform / delivery	org	not implemented	This organisation	—	—
5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server	org	implemented	This organisation	—	—
5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server	org	implemented	This organisation	—	—
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server	org	implemented	This organisation	—	—
8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that do not need the	Server	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	real values cannot see them.						
8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	Server	org	implemented	This organisation	—	—
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server	org	implemented	This organisation	—	—
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server	org	implemented	This organisation	—	—
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server	org	implemented	This organisation	—	—
8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server	org	implemented	This organisation	—	—
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	This organisation	—	—
8.25 Secure development life cycle	Establish and apply rules for the secure	Server	org	not implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	development of software and systems.						
8.26 Application security requirements	Identify, specify and approve information-security requirements for applications, including those that support transactions and payments.	Server	org	unknown	This organisation	—	—
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	This organisation	—	—
8.28 Secure coding	Apply secure coding principles to software development so common weaknesses are prevented.	Server	org	not implemented	This organisation	—	—
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	This organisation	—	—
8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server	org	implemented	This organisation	—	—
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	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
8.32 Change management	Control changes to information-processing facilities and systems through a documented change-management process.	Server	org	not implemented	This organisation	—	—
8.33 Test information	Select, protect and manage test information so production data is not improperly used or exposed in test.	Server	org	not implemented	This organisation	—	—
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	This organisation	—	—
8.4 Access to source code	Manage read and write access to source code, development tools and software libraries.	Server	org	not implemented	This organisation	—	—
5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server (access hop)	org	implemented	This organisation	—	—
5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server (access hop)	org	implemented	This organisation	—	—
5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server (access hop)	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server (access hop)	org	implemented	This organisation	—	—
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server (access hop)	org	implemented	This organisation	—	—
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server (access hop)	org	implemented	This organisation	—	—
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	This organisation	—	—
8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server (access hop)	org	implemented	This organisation	—	—
8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server (access hop)	org	implemented	This organisation	—	—
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	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
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	This organisation	—	—
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	This organisation	—	—
8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server (access hop)	org	implemented	This organisation	—	—
8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server (access hop)	org	implemented	This organisation	—	—
5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server → Bucket	org	implemented	This organisation	—	—
5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server → Bucket	org	implemented	This organisation	—	—
5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens)	Server → Bucket	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	throughout their life.						
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server → Bucket	org	implemented	This organisation	—	—
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server → Bucket	org	implemented	This organisation	—	—
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	Server → Bucket	org	implemented	This organisation	—	—
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server → Bucket	org	implemented	This organisation	—	—
8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server → Bucket	org	implemented	This organisation	—	—
8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server → Bucket	org	implemented	This organisation	—	—
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 → Bucket	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server → Bucket	org	implemented	This organisation	—	—
8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server → Bucket	org	implemented	This organisation	—	—
5.14 Information transfer	Protect information when it is transferred inside the organisation and with external parties.	Server → SQL	org	implemented	This organisation	—	—
5.15 Access control	Establish access-control rules based on business and security requirements, and apply them consistently.	Server → SQL	org	implemented	This organisation	—	—
5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	Server → SQL	org	implemented	This organisation	—	—
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	Server → SQL	org	implemented	This organisation	—	—
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	Server → SQL	org	implemented	This organisation	—	—
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous	Server → SQL	org	implemented	This organisation	—	—

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	behaviour and take appropriate action.						
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	Server → SQL	org	implemented	This organisation	—	—
8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	Server → SQL	org	implemented	This organisation	—	—
8.20 Network security	Secure networks, information systems and applications on those networks, including information in transit.	Server → SQL	org	implemented	This organisation	—	—
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 → SQL	org	implemented	This organisation	—	—
8.3 Information access restriction	Restrict access to information and other associated assets according to the access-control policy.	Server → SQL	org	implemented	This organisation	—	—
8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	Server → SQL	org	implemented	This organisation	—	—
5.15 Access control	Establish access-control rules based on business and security requirements, and	SQL	supplier	implemented	Vendor review — Google	SSO being used	ISO 27001 certification

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	apply them consistently.						
5.17 Authentication information	Allocate, protect and change authentication secrets (passwords, keys, tokens) throughout their life.	SQL	supplier	implemented	Vendor review — Google	SSO being used	ISO 27001 certification
5.18 Access rights	Provision, review and revoke access rights according to policy and when roles change.	SQL	supplier	implemented	Vendor review — Google	SSO being used	ISO 27001 certification
5.29 Information security during disruption	Maintain information security at an agreed level during disruption.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
5.30 ICT readiness for business continuity	Plan ICT so information-processing can continue, recover and meet availability objectives during disruption.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.11 Data masking	Mask or otherwise reduce sensitive data so people and systems that do not need the real values cannot see them.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.12 Data leakage prevention	Detect and prevent unauthorised disclosure of information through technical and organisational measures matched to the data.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.13 Information backup	Take copies of information, software and systems, and test restoration,	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	according to an agreed backup policy.						
8.14 Redundancy of information processing facilities	Implement sufficient redundancy of information-processing facilities to meet availability requirements.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.15 Logging	Produce, protect, retain and review logs of events that can support monitoring, investigation and evidence.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.16 Monitoring activities	Monitor networks, systems and applications for anomalous behaviour and take appropriate action.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.17 Clock synchronization	Synchronise clocks of information-processing systems to a trusted time source so events can be correlated.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.2 Privileged access rights	Restrict and manage privileged access rights, and monitor their use.	SQL	supplier	implemented	Vendor review — Google	SSO being used	ISO 27001 certification
8.24 Use of cryptography	Define and apply rules for effective use of cryptography, including key management, matched to the classification of the information.	SQL	supplier	implemented	Vendor review — Google	ISO 27001 certification	ISO 27001 certification
8.3 Information access restriction	Restrict access to information and other associated assets according	SQL	supplier	implemented	Vendor review — Google	SSO being used	ISO 27001 certification

Control	What this control requires	Component	Who	Implementation	Provenance	Comment	Technology
	to the access-control policy.						
8.5 Secure authentication	Authenticate users and systems with a mechanism whose strength matches the access being granted.	SQL	supplier	implemented	Vendor review — Google	SSO being used	ISO 27001 certification

4.1 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

5. Open Control Actions

Task	Owner	Effort	Component	Control type	Suggested remediation
Establish contractual security requirements with third party	Google	M	Bucket	Logging	Commission a vendor assessment for Google covering logging.
Establish contractual security requirements with third party	Google	M	Bucket	Backup and restore	Commission a vendor assessment for Google covering resilience.
Establish contractual security requirements with third party	Google	M	Bucket	Supplier assurance	Commission a vendor assessment for Google covering supplier.
Establish contractual security requirements with third party	Google	M	SQL	Authorization	Commission a vendor assessment for Google covering authorization.
Establish contractual security requirements with third party	Google	M	SQL	Data-at-rest protection	Commission a vendor assessment for Google covering data_at_rest.
Establish contractual security requirements with third party	Google	M	SQL	Logging	Commission a vendor assessment for Google covering logging.
Establish contractual security requirements with third party	Google	M	SQL	Backup and restore	Commission a vendor assessment for Google covering resilience.
Establish contractual security requirements	Google	M	SQL	Supplier assurance	Commission a vendor assessment for Google covering supplier.

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

Appendix A. Controls not in this assessment

These counts are distinct ISO/IEC 27002:2022 control ids, not component copies. In this assessment means the topic is on at least one in-scope place. Not applicable means the subject is missing (for example no people, no premises). Waiting means a scope fact is still unknown, so the control is not marked off.

In this assessment	Not applicable	Waiting on a scope fact	ISO 27002:2022 catalogue
70	23	0	93

Not applicable (the subject is missing, so the control is off)

Id	Title	What this control requires	Why
6.1	Screening	Screen personnel before hiring, and during employment when the role requires it, proportionate to the information they will access.	deliveryContext.workforceInScope=no
6.2	Terms and conditions of employment	State information-security responsibilities in employment terms and enforce them.	deliveryContext.workforceInScope=no

Id	Title	What this control requires	Why
6.3	Information security awareness, education and training	Provide information-security awareness, education and training appropriate to roles, and keep it current.	deliveryContext.workforceInScope=no
6.4	Disciplinary process	Apply a disciplinary process to information-security violations.	deliveryContext.workforceInScope=no
6.5	Responsibilities after termination or change of employment	After termination or role change, revoke access, recover assets and remind the person of ongoing confidentiality duties.	deliveryContext.workforceInScope=no
6.6	Confidentiality or non-disclosure agreements	Require confidentiality or non-disclosure agreements from personnel and relevant external parties who can access information.	deliveryContext.workforceInScope=no
6.7	Remote working	Implement security measures for remote working that protect information accessed, processed or stored outside organisation premises.	deliveryContext.workforceInScope=no
6.8	Information security event reporting	Provide a way for personnel to report observed or suspected information-security events in time.	deliveryContext.workforceInScope=no
7.1	Physical security perimeters	Define and use physical security perimeters to protect areas that contain information and processing facilities.	deliveryContext.premisesInScope=no
7.2	Physical entry	Control physical entry so only authorised people can enter secure areas.	deliveryContext.premisesInScope=no
7.3	Securing offices, rooms and facilities	Design and protect offices, rooms and facilities against unauthorised access, damage and interference.	deliveryContext.premisesInScope=no
7.4	Physical security monitoring	Monitor premises for unauthorised physical access.	deliveryContext.premisesInScope=no
7.5	Protecting against physical and environmental threats	Protect against physical and environmental threats such as fire, flood, earthquake, civil unrest and other physical damage.	deliveryContext.premisesInScope=no
7.6	Working in secure areas	Design and apply working practices for secure areas that prevent unauthorised access, damage and interference.	deliveryContext.premisesInScope=no
7.7	Clear desk and clear screen	Require clear desk and clear screen practices so information is not left exposed.	deliveryContext.premisesInScope=no
7.8	Equipment siting and protection	Site and protect equipment to reduce risks from environmental threats, unauthorised access and unauthorised viewing.	deliveryContext.premisesInScope=no
7.9	Security of assets off-premises	Protect assets used off-premises (including during transit) to the same standard as on-premises use requires.	deliveryContext.premisesInScope=no
7.10	Storage media	Manage storage media through its life, including acquisition, use, transport, reuse and disposal.	deliveryContext.premisesInScope=no

Id	Title	What this control requires	Why
7.11	Supporting utilities	Protect supporting utilities (power, cooling, water, communications) against failure, unauthorised access and tampering.	deliveryContext.premisesInScope=no
7.12	Cabling security	Protect power and data cabling from interception, interference and damage.	deliveryContext.premisesInScope=no
7.13	Equipment maintenance	Maintain equipment so availability, integrity and confidentiality are preserved.	deliveryContext.premisesInScope=no
7.14	Secure disposal or re-use of equipment	Sanitize or securely destroy equipment and storage media before reuse or disposal so information cannot be recovered.	deliveryContext.premisesInScope=no
8.30	Outsourced development	Direct, monitor and review outsourced system development so it meets the organisation's security requirements.	deliveryContext.softwareSourcing=custom_in_house

Waiting (a scope fact is still unknown, so the control is neither on nor off)

None recorded.

Generated by Riskonami from assessment data version v2. Vendor comments and technology are shown only after the organisation accepts that questionnaire.