ResolvX

Controls Owners Register

GRC Compliance & Audit Readiness | Phase 3 — Policy & Vendor Framework | Version 1.0

ISO/IEC 27001:2022 · SOC 2 TSC (AICPA) · NIST CSF 2.0 | Internal — Confidential

Document Information

Version	1.0
Status	Active
Classification	Internal — Confidential
Owner	GRC Lead — Derick G. Dmello
Phase	3 — Policy & Vendor Framework
Frameworks	ISO/IEC 27001:2022 · SOC 2 TSC · NIST CSF 2.0
Review Cycle	Quarterly, or following framework mapping updates
Last Updated	2026

Purpose

This register provides the inverted view of the three framework mappings, rather than showing controls with their owners, it shows each owner with the full portfolio of controls, criteria, and subcategories they are accountable for across ISO 27001:2022, SOC 2 TSC, and NIST CSF 2.0.

It is the definitive accountability document for ResolvX's ISMS. Each owner uses this register to understand their evidence obligations, review cadence, and Phase 3 policy responsibilities.

Control Owner Summary

Role	ISO 27001	SOC 2 TSC	NIST CSF 2.0	Total Controls
GRC Lead	41 controls	27 criteria	67 subcategories	**135**
CISO	8 controls	6 criteria	16 subcategories	**30**
IT Admin	22 controls	8 criteria	13 subcategories	**43**
Head of Cloud Ops	27 controls	10 criteria	27 subcategories	**64**
VP Engineering	12 controls	3 criteria	7 subcategories	**22**
DevSecOps	15 controls	3 criteria	11 subcategories	**29**
Head of HR	9 controls	5 criteria	4 subcategories	**18**
Legal	9 controls	9 criteria	8 subcategories	**26**

GRC Lead — GRC Lead

Name / Incumbent	Derick G. Dmello
Function	Owns the ISMS programme. Accountable for policy, risk, compliance, and audit readiness across all frameworks.
Total Controls	135 (41 ISO 27001 · 27 SOC 2 · 67 NIST CSF 2.0)
Review Cadence	Monthly — reviews control status, risk register, and evidence pipeline. Quarterly management reporting.
Phase 3 Policies	Information Security Policy, Acceptable Use Policy, Data Classification Policy, Vendor Management Policy, Privacy Programme (ROPA + DSR)

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.1	Policies for information security	→ Planned	Critical	Pending Review
5.2	Information security roles and responsibilities	✓ Implemented	High	Pending Review
5.3	Segregation of duties	~ Partial	High	Pending Review
5.5	Contact with authorities	→ Planned	Medium	Pending Review
5.6	Contact with special interest groups	→ Planned	Low	Pending Review
5.7	Threat intelligence	~ Partial	High	Pending Review
5.8	Information security in project management	→ Planned	Medium	Pending Review
5.10	Acceptable use of information and other associated assets	→ Planned	High	Pending Review
5.12	Classification of information	~ Partial	High	Pending Review
5.13	Labelling of information	→ Planned	Medium	Pending Review
5.14	Information transfer	~ Partial	High	Pending Review
5.19	Information security in supplier relationships	→ Planned	Critical	Pending Review
5.20	Addressing information security within supplier agreements	~ Partial	High	Pending Review
5.21	Managing information security in the ICT supply chain	→ Planned	High	Pending Review
5.22	Monitoring, review and change management of supplier services	→ Planned	High	Pending Review
5.23	Information security for use of cloud services	~ Partial	High	Pending Review
5.24	Information security incident management planning and preparation	→ Planned	Critical	Pending Review
5.25	Assessment and decision on information security events	→ Planned	High	Pending Review
5.26	Response to information security incidents	→ Planned	Critical	Pending Review

5.27	Learning from information security incidents	→ Planned	Medium	Pending Review
5.28	Collection of evidence	→ Planned	Medium	Pending Review
5.29	Information security during disruption	→ Planned	High	Pending Review
5.31	Legal, statutory, regulatory and contractual requirements	~ Partial	Critical	Pending Review
5.33	Protection of records	~ Partial	High	Pending Review
5.34	Privacy and protection of personal information	~ Partial	Critical	Pending Review
5.35	Independent review of information security	→ Planned	High	Pending Review
5.36	Compliance with policies, rules and standards for information security	→ Planned	High	Pending Review
6.3	Information security awareness, education and training	~ Partial	Critical	Pending Review
6.5	Responsibilities after termination or change of employment	~ Partial	High	Pending Review
6.8	Information security event reporting	→ Planned	High	Pending Review
7.1	Physical security perimeters	~ Partial	Medium	Pending Review
7.6	Working in secure areas	→ Planned	Low	Pending Review
7.7	Clear desk and clear screen	→ Planned	Medium	Pending Review
7.10	Storage media	~ Partial	Medium	Pending Review
8.10	Information deletion	→ Planned	High	Pending Review
8.12	Data leakage prevention	→ Planned	High	Pending Review
8.26	Application security requirements	→ Planned	High	Pending Review
8.30	Outsourced development	~ Partial	Medium	Pending Review
8.32	Change management	~ Partial	High	Pending Review
8.33	Test information	~ Partial	High	Pending Review
8.34	Protection of information systems during audit testing	→ Planned	Medium	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
CC1.3	COSO Principle 3 — Organisational Structure	✓ Implemented
CC1.4	COSO Principle 4 — Commitment to Competence	~ Partial
CC2.1	COSO Principle 13 — Relevant, Quality Information	~ Partial
CC2.2	COSO Principle 14 — Internal Communication	~ Partial
CC2.3	COSO Principle 15 — External Communication	~ Partial
CC3.1	COSO Principle 6 — Appropriate Objectives	✓ Implemented
CC3.2	COSO Principle 7 — Risk Identification & Analysis	✓ Implemented
CC3.3	COSO Principle 8 — Fraud Risk	~ Partial

CC3.4	COSO Principle 9 — Change Identification & Analysis	→ Planned
CC4.1	COSO Principle 16 — Ongoing Evaluations	→ Planned
CC4.2	COSO Principle 17 — Communication of Deficiencies	→ Planned
CC5.1	COSO Principle 10 — Control Activities	~ Partial
CC5.3	COSO Principle 12 — Policy Deployment	→ Planned
CC7.3	System Operations — Event Evaluation	→ Planned
CC7.4	System Operations — Incident Response	→ Planned
CC7.5	System Operations — Post-Incident Recovery	→ Planned
CC8.1	Change Management	~ Partial
CC9.1	Risk Mitigation — Vendor Risk	→ Planned
CC9.2	Risk Mitigation — Business Partner Risk	~ Partial
P1.1	Privacy — Notice	~ Partial
P2.1	Privacy — Choice & Consent	~ Partial
P3.1	Privacy — Collection	→ Planned
P4.1	Privacy — Use, Retention & Disposal	→ Planned
P5.1	Privacy — Access	→ Planned
P6.1	Privacy — Disclosure & Notification	~ Partial
P7.1	Privacy — Quality	→ Planned
P8.1	Privacy — Monitoring & Enforcement	→ Planned

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
DE.AE-02	DETECT	Potentially adverse events are analysed to better understand associated activities.	→ Planned
DE.AE-04	DETECT	The estimated impact and scope of adverse events are understood.	→ Planned
DE.AE-07	DETECT	Cyber threat intelligence and other contextual information are integrated into the analysis of adverse events.	→ Planned
DE.AE-08	DETECT	Incidents are declared when adverse events meet the defined criteria.	→ Planned
DE.CM-06	DETECT	External service provider activities and services are monitored to detect potential adverse events.	→ Planned
GV.OC-01	GOVERN	The organizational mission is understood and informs cybersecurity risk management.	✓ Implemented
GV.OC-02	GOVERN	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity ar…	✓ Implemented
GV.OC-03	GOVERN	Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties…	~ Partial
GV.OC-04	GOVERN	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organi…	~ Partial
GV.OC-05	GOVERN	Outcomes, capabilities, and services that the organization depends on are understood and communicated.	~ Partial

GV.OV-01	GOVERN	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	→ Planned
GV.OV-03	GOVERN	Organisational cybersecurity risk management performance is evaluated and reviewed for adherence to the risk m…	→ Planned
GV.PO-01	GOVERN	Policy for managing cybersecurity risks is established based on organisational context, cybersecurity strategy…	→ Planned
GV.PO-02	GOVERN	Policy is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology…	→ Planned
GV.RM-01	GOVERN	The organizational risk management objectives are established and agreed to by organizational stakeholders.	✓ Implemented
GV.RM-02	GOVERN	Risk appetite and risk tolerance statements are established, communicated, and maintained.	✓ Implemented
GV.RM-03	GOVERN	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	~ Partial
GV.RM-04	GOVERN	Strategic direction that describes appropriate risk response options is established and communicated.	✓ Implemented
GV.RM-05	GOVERN	Lines of communication across the organisation are established for cybersecurity risks, including risks from s…	~ Partial
GV.RM-06	GOVERN	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is esta…	✓ Implemented
GV.RM-07	GOVERN	Strategic opportunities (positive risks) are characterised and included in organisational cybersecurity risk d…	→ Planned
GV.RR-02	GOVERN	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicate…	✓ Implemented
GV.RR-04	GOVERN	Cybersecurity is included in human resources practices.	~ Partial
GV.SC-01	GOVERN	A cybersecurity supply chain risk management programme, strategy, objectives, policies, and processes are esta…	→ Planned
GV.SC-02	GOVERN	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated,…	~ Partial
GV.SC-03	GOVERN	Suppliers are known and prioritised by criticality.	✓ Implemented
GV.SC-04	GOVERN	Suppliers are routinely assessed using audits, test results, or other forms of evaluations to confirm they are…	→ Planned
GV.SC-05	GOVERN	Requirements to address cybersecurity risks in supply chains are established, prioritised, and integrated into…	~ Partial
GV.SC-06	GOVERN	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-p…	→ Planned
GV.SC-07	GOVERN	The risks posed by a supplier, their products and services, and other third parties are understood and recorde…	~ Partial
GV.SC-08	GOVERN	Relevant suppliers and other third parties are included in incident response planning.	→ Planned
GV.SC-09	GOVERN	Supply chain security practices are integrated into cybersecurity and enterprise risk management programmes, p…	→ Planned
GV.SC-10	GOVERN	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclu…	→ Planned
ID.AM-04	IDENTIFY	Inventories of services provided by suppliers are maintained.	✓ Implemented

ID.AM-05	IDENTIFY	Assets are prioritised based on classification, criticality, resources, and impact on mission.	✓ Implemented
ID.AM-07	IDENTIFY	Inventories of data and corresponding metadata for designated data types are maintained.	→ Planned
ID.IM-01	IDENTIFY	Improvements are identified from evaluations — including tests, exercises, assessments, and lessons learned.	→ Planned
ID.IM-02	IDENTIFY	Improvements are identified from security tests and exercises, including those done in collaboration with supp…	→ Planned
ID.IM-03	IDENTIFY	Improvements are identified from execution of operational processes, including incident response.	→ Planned
ID.IM-04	IDENTIFY	Incident, vulnerability, and other findings are communicated to those responsible for addressing them.	~ Partial
ID.RA-02	IDENTIFY	Cyber threat intelligence is received from information sharing forums and sources.	~ Partial
ID.RA-03	IDENTIFY	Internal and external threats to the organisation are identified and recorded.	✓ Implemented
ID.RA-04	IDENTIFY	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	✓ Implemented
ID.RA-05	IDENTIFY	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk respon…	✓ Implemented
ID.RA-06	IDENTIFY	Risk responses are chosen, prioritised, planned, tracked, and communicated to stakeholders.	~ Partial
ID.RA-07	IDENTIFY	Changes and exceptions are managed, assessed for risk impact, informed by risk assessments, and recorded.	→ Planned
PR.AT-01	PROTECT	Personnel are provided awareness and training so that they possess knowledge and skills to perform general tas…	~ Partial
PR.AT-02	PROTECT	Individuals in specialised roles are provided with awareness and training so that they possess the knowledge a…	~ Partial
RC.CO-03	RECOVER	Recovery activities and progress in restoring operational capabilities are communicated to internal and extern…	→ Planned
RC.CO-04	RECOVER	Public updates on incident recovery are shared using approved methods and messages.	→ Planned
RC.RP-01	RECOVER	The recovery portion of the incident response plan is executed once initiated by appropriate personnel.	→ Planned
RC.RP-02	RECOVER	Recovery actions are selected, scoped, prioritised, and performed.	→ Planned
RC.RP-04	RECOVER	Critical mission functions and cybersecurity risk management are considered to establish post-incident operati…	→ Planned
RC.RP-06	RECOVER	The end of incident recovery is declared based on criteria, and incident-related documentation is completed.	→ Planned
RS.AN-03	RESPOND	Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	→ Planned
RS.AN-06	RESPOND	Actions performed during an investigation are recorded to preserve the integrity of the investigation.	→ Planned
RS.AN-07	RESPOND	Incident cause is determined and recorded.	→ Planned
RS.AN-08	RESPOND	Incidents are categorised consistent with the response plans.	→ Planned

RS.CO-02	RESPOND	Internal and external stakeholders are notified of incidents in a timely manner.	→ Planned
RS.CO-03	RESPOND	Information is shared with designated internal and external stakeholders consistent with the response plans.	→ Planned
RS.MA-01	RESPOND	The incident response plan is executed in coordination with relevant third parties once an incident is declare…	→ Planned
RS.MA-02	RESPOND	Incident reports are triaged and validated.	→ Planned
RS.MA-03	RESPOND	Incidents are categorised and prioritised.	→ Planned
RS.MA-04	RESPOND	Incidents are escalated or elevated as needed.	~ Partial
RS.MA-05	RESPOND	The criteria for initiating incident recovery are applied.	→ Planned
RS.MI-01	RESPOND	Incidents are contained.	→ Planned
RS.MI-02	RESPOND	Incidents are eradicated.	→ Planned

CISO — Chief Information Security Officer

Name / Incumbent	TBA / Interim: GRC Lead
Function	Executive accountability for ResolvX's security posture. Approves policies, escalates material risks, and interfaces with board.
Total Controls	30 (8 ISO 27001 · 6 SOC 2 · 16 NIST CSF 2.0)
Review Cadence	Quarterly — reviews programme status, approves policy changes, signs off on risk acceptance decisions.
Phase 3 Policies	Information Security Policy (approval authority)

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.4	Management responsibilities	→ Planned	Medium	Pending Review
5.35	Independent review of information security	→ Planned	High	Pending Review
7.1	Physical security perimeters	~ Partial	Medium	Pending Review
7.2	Physical entry	~ Partial	Low	Pending Review
7.3	Securing offices, rooms and facilities	~ Partial	Low	Pending Review
7.4	Physical security monitoring	~ Partial	Low	Pending Review
7.6	Working in secure areas	→ Planned	Low	Pending Review
8.34	Protection of information systems during audit testing	→ Planned	Medium	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
CC1.1	COSO Principle 1 — Integrity & Ethical Values	~ Partial
CC1.2	COSO Principle 2 — Board Oversight	~ Partial
CC1.5	COSO Principle 5 — Enforcement of Accountability	~ Partial
CC4.1	COSO Principle 16 — Ongoing Evaluations	→ Planned
CC6.4	Physical Access Restrictions	~ Partial
CC7.4	System Operations — Incident Response	→ Planned

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
DE.CM-02	DETECT	The physical environment is monitored to find potentially adverse events.	~ Partial
GV.OV-01	GOVERN	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	→ Planned
GV.OV-02	GOVERN	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organisational requi…	→ Planned

GV.OV-03	GOVERN	Organisational cybersecurity risk management performance is evaluated and reviewed for adherence to the risk m…	→ Planned
GV.RM-01	GOVERN	The organizational risk management objectives are established and agreed to by organizational stakeholders.	✓ Implemented
GV.RM-02	GOVERN	Risk appetite and risk tolerance statements are established, communicated, and maintained.	✓ Implemented
GV.RM-03	GOVERN	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	~ Partial
GV.RM-05	GOVERN	Lines of communication across the organisation are established for cybersecurity risks, including risks from s…	~ Partial
GV.RR-01	GOVERN	Organisational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is …	~ Partial
GV.RR-03	GOVERN	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, a…	~ Partial
PR.AA-06	PROTECT	Physical access to assets is managed, monitored, and enforced commensurate with risk.	~ Partial
PR.IR-04	PROTECT	Adequate resource capacity is ensured to support cybersecurity.	~ Partial
RC.CO-03	RECOVER	Recovery activities and progress in restoring operational capabilities are communicated to internal and extern…	→ Planned
RC.CO-04	RECOVER	Public updates on incident recovery are shared using approved methods and messages.	→ Planned
RS.MA-01	RESPOND	The incident response plan is executed in coordination with relevant third parties once an incident is declare…	→ Planned
RS.MA-04	RESPOND	Incidents are escalated or elevated as needed.	~ Partial

IT Admin — IT Administrator

Name / Incumbent	IT Administrator
Function	Owns identity, endpoint, and access management controls. Manages Okta, Jamf MDM, and 1Password deployment.
Total Controls	43 (22 ISO 27001 · 8 SOC 2 · 13 NIST CSF 2.0)
Review Cadence	Monthly — access review cycle, MDM compliance reports, MFA enforcement status.
Phase 3 Policies	Access Control Policy (primary owner)

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.3	Segregation of duties	**~ Partial**	High	Pending Review
5.11	Return of assets	**~ Partial**	High	Pending Review
5.13	Labelling of information	**→ Planned**	Medium	Pending Review
5.15	Access control	**~ Partial**	Critical	Pending Review
5.16	Identity management	**~ Partial**	High	Pending Review
5.17	Authentication information	**~ Partial**	High	Pending Review
5.18	Access rights	**→ Planned**	Critical	Pending Review
6.7	Remote working	**✓ Implemented**	High	Pending Review
7.8	Equipment siting and protection	**✓ Implemented**	Medium	Pending Review
7.9	Security of assets off-premises	**✓ Implemented**	High	Pending Review
7.10	Storage media	**~ Partial**	Medium	Pending Review
7.13	Equipment maintenance	**✓ Implemented**	Medium	Pending Review
7.14	Secure disposal or re-use of equipment	**→ Planned**	Medium	Pending Review
8.1	User end point devices	**✓ Implemented**	High	Pending Review
8.2	Privileged access rights	**~ Partial**	Critical	Pending Review
8.3	Information access restriction	**~ Partial**	Critical	Pending Review
8.5	Secure authentication	**✓ Implemented**	Critical	Pending Review
8.7	Protection against malware	**✓ Implemented**	Critical	Pending Review
8.12	Data leakage prevention	**→ Planned**	High	Pending Review
8.18	Use of privileged utility programs	**~ Partial**	High	Pending Review
8.19	Installation of software on operational systems	**~ Partial**	High	Pending Review
8.23	Web filtering	**→ Planned**	Medium	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status

CC5.2	COSO Principle 11 — Technology General Controls	**~ Partial**
CC6.1	Logical Access — Infrastructure & Software	**~ Partial**
CC6.2	Logical Access — Prior to Issuance	**~ Partial**
CC6.3	Logical Access — Removes Access	**~ Partial**
CC6.5	Logical Access — Disposal	**~ Partial**
CC6.6	Logical Access — External Threats	**✓ Implemented**
CC6.7	Logical Access — Transmission & Removal	**~ Partial**
CC6.8	Logical Access — Malicious Software	**✓ Implemented**

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
DE.CM-03	DETECT	Personnel activity and technology usage are monitored to find potentially adverse events.	**~ Partial**
ID.AM-01	IDENTIFY	Inventories of hardware managed by the organisation are maintained.	**✓ Implemented**
ID.AM-02	IDENTIFY	Inventories of software, services, and systems managed by the organisation are maintained.	**✓ Implemented**
ID.AM-08	IDENTIFY	Systems, hardware, software, services, and data are managed throughout their life cycles.	**~ Partial**
PR.AA-01	PROTECT	Identities and credentials for authorised users, services, and hardware are managed by the organisation.	**~ Partial**
PR.AA-02	PROTECT	Identities are proofed and bound to credentials based on the context of interactions.	**~ Partial**
PR.AA-03	PROTECT	Users, services, and hardware are authenticated.	**✓ Implemented**
PR.AA-04	PROTECT	Identity assertions are protected, conveyed, and verified.	**✓ Implemented**
PR.AA-05	PROTECT	Access permissions, entitlements, and authorisations are defined in a policy, managed, and enforced commensura…	**~ Partial**
PR.DS-01	PROTECT	The confidentiality, integrity, and availability of data-at-rest are protected.	**✓ Implemented**
PR.PS-02	PROTECT	Software is maintained, replaced, and removed commensurate with risk.	**~ Partial**
PR.PS-03	PROTECT	Hardware is maintained, replaced, and removed commensurate with risk.	**~ Partial**
PR.PS-05	PROTECT	Installation and execution of unauthorised software are prevented.	**~ Partial**

Head of Cloud Ops — Head of Cloud Operations

Name / Incumbent	Head of Cloud Operations
Function	Owns AWS infrastructure security, logging, monitoring, backup, and availability controls.
Total Controls	64 (27 ISO 27001 · 10 SOC 2 · 27 NIST CSF 2.0)
Review Cadence	Monthly — CloudTrail review, GuardDuty alerts, backup test status, capacity utilisation.

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.9	Inventory of information and other associated assets	✓ Implemented	High	Pending Review
5.23	Information security for use of cloud services	~ Partial	High	Pending Review
5.25	Assessment and decision on information security events	→ Planned	High	Pending Review
5.33	Protection of records	~ Partial	High	Pending Review
5.37	Documented operating procedures	~ Partial	Medium	Pending Review
7.5	Protecting against physical and environmental threats	~ Partial	Medium	Pending Review
7.8	Equipment siting and protection	✓ Implemented	Medium	Pending Review
7.11	Supporting utilities	✓ Implemented	Medium	Pending Review
7.12	Cabling security	✓ Implemented	Low	Pending Review
7.13	Equipment maintenance	✓ Implemented	Medium	Pending Review
8.2	Privileged access rights	~ Partial	Critical	Pending Review
8.3	Information access restriction	~ Partial	Critical	Pending Review
8.6	Capacity management	~ Partial	Medium	Pending Review
8.9	Configuration management	~ Partial	High	Pending Review
8.10	Information deletion	→ Planned	High	Pending Review
8.11	Data masking	~ Partial	High	Pending Review
8.13	Information backup	~ Partial	Critical	Pending Review
8.14	Redundancy of information processing facilities	~ Partial	High	Pending Review
8.15	Logging	~ Partial	Critical	Pending Review
8.16	Monitoring activities	~ Partial	Critical	Pending Review
8.17	Clock synchronization	✓ Implemented	Low	Pending Review
8.18	Use of privileged utility programs	~ Partial	High	Pending Review
8.20	Networks security	~ Partial	High	Pending Review
8.21	Security of network services	~ Partial	High	Pending Review

8.22	Segregation of networks	**~ Partial**	High	Pending Review
8.24	Use of cryptography	**~ Partial**	High	Pending Review
8.31	Separation of development, test and production environments	**✓ Implemented**	High	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
A1.1	Availability — Capacity & Performance	**~ Partial**
A1.2	Availability — Recovery	**~ Partial**
A1.3	Availability — Environmental Threats	**✓ Implemented**
CC5.2	COSO Principle 11 — Technology General Controls	**~ Partial**
CC6.1	Logical Access — Infrastructure & Software	**~ Partial**
CC6.5	Logical Access — Disposal	**~ Partial**
CC6.7	Logical Access — Transmission & Removal	**~ Partial**
CC7.1	System Operations — Detection & Monitoring	**~ Partial**
CC7.2	System Operations — Anomaly Monitoring	**~ Partial**
P4.1	Privacy — Use, Retention & Disposal	**→ Planned**

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
DE.AE-02	DETECT	Potentially adverse events are analysed to better understand associated activities.	**→ Planned**
DE.AE-03	DETECT	Information is correlated from multiple sources.	**→ Planned**
DE.AE-06	DETECT	Information on adverse events is provided to authorised staff and tools.	**~ Partial**
DE.CM-01	DETECT	Networks and network services are monitored to find potentially adverse events.	**~ Partial**
DE.CM-03	DETECT	Personnel activity and technology usage are monitored to find potentially adverse events.	**~ Partial**
DE.CM-06	DETECT	External service provider activities and services are monitored to detect potential adverse events.	**→ Planned**
DE.CM-09	DETECT	Computing hardware and software, runtime environments, and their data are monitored to find potentially advers…	**~ Partial**
ID.AM-02	IDENTIFY	Inventories of software, services, and systems managed by the organisation are maintained.	**✓ Implemented**
ID.AM-03	IDENTIFY	Representations of network communication and data flows are maintained.	**~ Partial**
ID.AM-05	IDENTIFY	Assets are prioritised based on classification, criticality, resources, and impact on mission.	**✓ Implemented**
ID.AM-08	IDENTIFY	Systems, hardware, software, services, and data are managed throughout their life cycles.	**~ Partial**

PR.AA-05	PROTECT	Access permissions, entitlements, and authorisations are defined in a policy, managed, and enforced commensura…	**~ Partial**
PR.DS-01	PROTECT	The confidentiality, integrity, and availability of data-at-rest are protected.	**✓ Implemented**
PR.DS-02	PROTECT	The confidentiality, integrity, and availability of data-in-transit are protected.	**✓ Implemented**
PR.DS-10	PROTECT	The confidentiality, integrity, and availability of data-in-use are protected.	**→ Planned**
PR.DS-11	PROTECT	Backups of data are created, protected, maintained, and tested.	**~ Partial**
PR.IR-01	PROTECT	Networks and environments are protected from unauthorised logical access and usage.	**~ Partial**
PR.IR-02	PROTECT	The organisation's technology assets are protected from environmental threats.	**✓ Implemented**
PR.IR-03	PROTECT	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	**~ Partial**
PR.IR-04	PROTECT	Adequate resource capacity is ensured to support cybersecurity.	**~ Partial**
PR.PS-01	PROTECT	Configuration management practices are established and applied.	**~ Partial**
PR.PS-03	PROTECT	Hardware is maintained, replaced, and removed commensurate with risk.	**~ Partial**
PR.PS-04	PROTECT	Log records are created to enable monitoring, forensics, investigations, and incident response support.	**~ Partial**
RC.RP-03	RECOVER	The integrity of backups and other restoration assets is verified before using them in restoration.	**→ Planned**
RC.RP-05	RECOVER	The integrity of restored assets is verified, systems and services are restored, and normal operating status i…	**→ Planned**
RS.AN-03	RESPOND	Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	**→ Planned**
RS.MI-01	RESPOND	Incidents are contained.	**→ Planned**

VP Engineering — VP of Engineering

Name / Incumbent	VP of Engineering
Function	Owns secure development lifecycle, environment separation, change management, and ICT continuity controls.
Total Controls	22 (12 ISO 27001 · 3 SOC 2 · 7 NIST CSF 2.0)
Review Cadence	Quarterly — secure coding compliance, change management log review, DR readiness.

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.8	Information security in project management	→ Planned	Medium	Pending Review
5.29	Information security during disruption	→ Planned	High	Pending Review
5.30	ICT readiness for business continuity	~ Partial	High	Pending Review
5.32	Intellectual property rights	~ Partial	Low	Pending Review
8.4	Access to source code	✓ Implemented	High	Pending Review
8.14	Redundancy of information processing facilities	~ Partial	High	Pending Review
8.25	Secure development life cycle	~ Partial	High	Pending Review
8.26	Application security requirements	→ Planned	High	Pending Review
8.27	Secure system architecture and engineering principles	→ Planned	High	Pending Review
8.30	Outsourced development	~ Partial	Medium	Pending Review
8.31	Separation of development, test and production environments	✓ Implemented	High	Pending Review
8.32	Change management	~ Partial	High	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
A1.2	Availability — Recovery	~ Partial
CC7.5	System Operations — Post-Incident Recovery	→ Planned
CC8.1	Change Management	~ Partial

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
GV.OC-04	GOVERN	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organi…	~ Partial
PR.IR-03	PROTECT	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	~ Partial

PR.PS-06	PROTECT	Secure software development practices are integrated, and their security is evaluated.	**~ Partial**
RC.RP-01	RECOVER	The recovery portion of the incident response plan is executed once initiated by appropriate personnel.	**→ Planned**
RC.RP-02	RECOVER	Recovery actions are selected, scoped, prioritised, and performed.	**→ Planned**
RC.RP-04	RECOVER	Critical mission functions and cybersecurity risk management are considered to establish post-incident operati…	**→ Planned**
RS.MA-05	RESPOND	The criteria for initiating incident recovery are applied.	**→ Planned**

DevSecOps — DevSecOps Engineer

Name / Incumbent	DevSecOps Engineer
Function	Owns vulnerability management, SAST/DAST tooling, secrets management, and CI/CD security controls.
Total Controls	29 (15 ISO 27001 · 3 SOC 2 · 11 NIST CSF 2.0)
Review Cadence	Monthly — vulnerability scan results, patch SLA compliance, container scan reports.

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.21	Managing information security in the ICT supply chain	→ Planned	High	Pending Review
5.28	Collection of evidence	→ Planned	Medium	Pending Review
8.4	Access to source code	✓ Implemented	High	Pending Review
8.7	Protection against malware	✓ Implemented	Critical	Pending Review
8.8	Management of technical vulnerabilities	~ Partial	Critical	Pending Review
8.9	Configuration management	~ Partial	High	Pending Review
8.11	Data masking	~ Partial	High	Pending Review
8.16	Monitoring activities	~ Partial	Critical	Pending Review
8.19	Installation of software on operational systems	~ Partial	High	Pending Review
8.24	Use of cryptography	~ Partial	High	Pending Review
8.25	Secure development life cycle	~ Partial	High	Pending Review
8.27	Secure system architecture and engineering principles	→ Planned	High	Pending Review
8.28	Secure coding	~ Partial	High	Pending Review
8.29	Security testing in development and acceptance	~ Partial	High	Pending Review
8.33	Test information	~ Partial	High	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
CC6.6	Logical Access — External Threats	✓ Implemented
CC6.8	Logical Access — Malicious Software	✓ Implemented
CC7.1	System Operations — Detection & Monitoring	~ Partial

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status

DE.CM-09	DETECT	Computing hardware and software, runtime environments, and their data are monitored to find potentially advers…	**~ Partial**
GV.SC-09	GOVERN	Supply chain security practices are integrated into cybersecurity and enterprise risk management programmes, p…	**→ Planned**
ID.IM-02	IDENTIFY	Improvements are identified from security tests and exercises, including those done in collaboration with supp…	**→ Planned**
ID.RA-01	IDENTIFY	Vulnerabilities in assets are identified, validated, and recorded.	**~ Partial**
PR.DS-10	PROTECT	The confidentiality, integrity, and availability of data-in-use are protected.	**→ Planned**
PR.PS-01	PROTECT	Configuration management practices are established and applied.	**~ Partial**
PR.PS-02	PROTECT	Software is maintained, replaced, and removed commensurate with risk.	**~ Partial**
PR.PS-05	PROTECT	Installation and execution of unauthorised software are prevented.	**~ Partial**
PR.PS-06	PROTECT	Secure software development practices are integrated, and their security is evaluated.	**~ Partial**
RC.RP-05	RECOVER	The integrity of restored assets is verified, systems and services are restored, and normal operating status i…	**→ Planned**
RS.MI-02	RESPOND	Incidents are eradicated.	**→ Planned**

Head of HR — Head of Human Resources

Name / Incumbent	Head of Human Resources
Function	Owns personnel security controls — screening, NDAs, security awareness training, offboarding, and disciplinary processes.
Total Controls	18 (9 ISO 27001 · 5 SOC 2 · 4 NIST CSF 2.0)
Review Cadence	Quarterly — training completion rates, offboarding checklist compliance, NDA register review.

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.11	Return of assets	**~ Partial**	High	Pending Review
6.1	Screening	**~ Partial**	High	Pending Review
6.2	Terms and conditions of employment	**~ Partial**	High	Pending Review
6.3	Information security awareness, education and training	**~ Partial**	Critical	Pending Review
6.4	Disciplinary process	**→ Planned**	Medium	Pending Review
6.5	Responsibilities after termination or change of employment	**~ Partial**	High	Pending Review
6.6	Confidentiality or non-disclosure agreements	**✓ Implemented**	High	Pending Review
7.3	Securing offices, rooms and facilities	**~ Partial**	Low	Pending Review
7.7	Clear desk and clear screen	**→ Planned**	Medium	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
CC1.1	COSO Principle 1 — Integrity & Ethical Values	**~ Partial**
CC1.4	COSO Principle 4 — Commitment to Competence	**~ Partial**
CC1.5	COSO Principle 5 — Enforcement of Accountability	**~ Partial**
CC2.2	COSO Principle 14 — Internal Communication	**~ Partial**
CC6.3	Logical Access — Removes Access	**~ Partial**

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
GV.RR-04	GOVERN	Cybersecurity is included in human resources practices.	**~ Partial**
PR.AA-02	PROTECT	Identities are proofed and bound to credentials based on the context of interactions.	**~ Partial**
PR.AT-01	PROTECT	Personnel are provided awareness and training so that they possess knowledge and skills to perform general tas…	**~ Partial**

PR.AT-02	PROTECT	Individuals in specialised roles are provided with awareness and training so that they possess the knowledge a…	**~ Partial**

Legal — Legal Counsel (Internal / External)

Name / Incumbent	Legal Counsel
Function	Owns contractual, regulatory, and privacy obligations. Reviews vendor agreements, DPAs, and compliance obligations register.
Total Controls	26 (9 ISO 27001 · 9 SOC 2 · 8 NIST CSF 2.0)
Review Cadence	Quarterly — DPA review cycle, regulatory change monitoring, privacy programme status.
Phase 3 Policies	Privacy Programme (co-owner)

ISO 27001:2022 Controls

ID	Control Name	Status	Priority	Evidence Status
5.5	Contact with authorities	→ Planned	Medium	Pending Review
5.14	Information transfer	~ Partial	High	Pending Review
5.20	Addressing information security within supplier agreements	~ Partial	High	Pending Review
5.31	Legal, statutory, regulatory and contractual requirements	~ Partial	Critical	Pending Review
5.32	Intellectual property rights	~ Partial	Low	Pending Review
5.34	Privacy and protection of personal information	~ Partial	Critical	Pending Review
6.2	Terms and conditions of employment	~ Partial	High	Pending Review
6.4	Disciplinary process	→ Planned	Medium	Pending Review
6.6	Confidentiality or non-disclosure agreements	✓ Implemented	High	Pending Review

SOC 2 TSC Criteria

TSC ID	Criterion Name	Status
CC2.3	COSO Principle 15 — External Communication	~ Partial
CC3.3	COSO Principle 8 — Fraud Risk	~ Partial
CC9.2	Risk Mitigation — Business Partner Risk	~ Partial
P1.1	Privacy — Notice	~ Partial
P2.1	Privacy — Choice & Consent	~ Partial
P3.1	Privacy — Collection	→ Planned
P5.1	Privacy — Access	→ Planned
P6.1	Privacy — Disclosure & Notification	~ Partial
P8.1	Privacy — Monitoring & Enforcement	→ Planned

NIST CSF 2.0 Subcategories

ID	Function	Subcategory Description	Status
GV.OC-03	GOVERN	Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties…	**~ Partial**
GV.SC-02	GOVERN	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated,…	**~ Partial**
GV.SC-05	GOVERN	Requirements to address cybersecurity risks in supply chains are established, prioritised, and integrated into…	**~ Partial**
GV.SC-10	GOVERN	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclu…	**→ Planned**
ID.AM-07	IDENTIFY	Inventories of data and corresponding metadata for designated data types are maintained.	**→ Planned**
RC.CO-04	RECOVER	Public updates on incident recovery are shared using approved methods and messages.	**→ Planned**
RS.CO-02	RESPOND	Internal and external stakeholders are notified of incidents in a timely manner.	**→ Planned**
RS.CO-03	RESPOND	Information is shared with designated internal and external stakeholders consistent with the response plans.	**→ Planned**

Document Control

Version	1.0
Status	Active
Owner	GRC Lead — Derick G. Dmello
Classification	Internal — Confidential
Review Cycle	Quarterly, or following framework mapping updates
Next Review	Q2 2026
Frameworks	ISO/IEC 27001:2022 · SOC 2 TSC (AICPA) · NIST CSF 2.0
Related Documents	ISO 27001 Control Matrix, SOC 2 TSC Mapping, NIST CSF 2.0 Mapping, Stakeholder Register