ISO/IEC 27001:2022 Statement of Applicability

All 93 Annex A controls — worked example for a 100-staff Australian B2B SaaS

Every control must be marked applicable or excluded, and every exclusion needs a scope-based justification an auditor will accept. Two controls are excluded in this example; the reasons are shown in full. Replace the justification column with your own environment.

THEME	CONTROL	CONTROL NAME	APPLICABLE	JUSTIFICATION / HOW IT IS IMPLEMENTED	IMPLEMENTATION STATUS	CONTROL OWNER
Organizational	A.5.1	Policies for information security	Yes	ISMS policy set approved by the board and reviewed annually. Published in SharePoint with read receipts tracked for all staff.	Implemented	
Organizational	A.5.2	Information security roles and responsibilities	Yes	Roles defined in the ISMS Manual: CTO as ISMS owner, Security Lead for day-to-day operation, control owners named per Annex A theme.	Implemented	
Organizational	A.5.3	Segregation of duties	Yes	Segregation enforced in Azure DevOps: authors cannot approve their own pull requests; production deploys need a second approver.	Implemented	
Organizational	A.5.4	Management responsibilities	Yes	Security responsibilities written into position descriptions and the employment contract; breaches handled under the disciplinary policy.	Implemented	
Organizational	A.5.5	Contact with authorities	Yes	Contact register maintained for the ACSC, the OAIC (for NDB reporting) and the state police cyber units.	Implemented	
Organizational	A.5.6	Contact with special interest groups	Yes	Membership of AISA and the ACSC Partnership Program; threat advisories reviewed at the fortnightly security stand-up.	Implemented	
Organizational	A.5.7	Threat intelligence	Yes	ACSC alerts and Microsoft Defender Threat Intelligence feed the monthly risk review; material items raised as risks within five working days.	Implemented	
Organizational	A.5.8	Information security in project management	Yes	Security requirements are a gate in the project intake template; no project reaches build without a completed security review.	Implemented	
Organizational	A.5.9	Inventory of information and other associated assets	Yes	Asset inventory maintained in Intune and Entra ID for endpoints and identities, and in Azure Resource Graph for cloud assets. Reconciled quarterly.	Implemented	
Organizational	A.5.10	Acceptable use of information and other associated assets	Yes	Acceptable Use Policy acknowledged at induction and re-acknowledged annually; enforced technically through Intune compliance policies.	Implemented	
Organizational	A.5.11	Return of assets	Yes	Offboarding checklist covers device return, Entra ID disablement and token revocation, with HR sign-off within one business day of exit.	Implemented	
Organizational	A.5.12	Classification of information	Yes	Four-tier scheme (Public / Internal / Confidential / Customer Data) implemented as Microsoft Purview sensitivity labels.	Implemented	
Organizational	A.5.13	Labelling of information	Yes	Purview labels apply visual markings and metadata automatically; auto-labelling policies cover customer data in SharePoint and Exchange.	Implemented	
Organizational	A.5.14	Information transfer	Yes	Transfer rules documented for customer data. TLS 1.2+ enforced in transit; external sharing restricted to authenticated guests.	Implemented	
Organizational	A.5.15	Access control	Yes	Role-based access model documented per system, with access matrices reviewed quarterly by system owners.	Implemented	
Organizational	A.5.16	Identity management	Yes	Entra ID is the single identity provider. Joiner-mover-leaver process is automated from the HRIS.	Implemented	
Organizational	A.5.17	Authentication information	Yes	Phishing-resistant MFA required for all staff; passwordless via Windows Hello and FIDO2 keys for privileged roles.	Implemented	
Organizational	A.5.18	Access rights	Yes	Access rights provisioned by group membership, reviewed quarterly, and revoked automatically on termination through HRIS integration.	Implemented	
Organizational	A.5.19	Information security in supplier relationships	Yes	Supplier security requirements in the standard MSA; security schedule mandatory for suppliers touching customer data.	Implemented	
Organizational	A.5.20	Addressing information security within supplier agreements	Yes	Security clauses in all supplier agreements covering incident notification within 24 hours, data location and audit rights.	Implemented	
Organizational	A.5.21	Managing information security in the ICT supply chain	Yes	Sub-processor register maintained and published; changes notified to customers 30 days ahead per contract.	Implemented	

THEME	CONTROL	CONTROL NAME	APPLICABLE	JUSTIFICATION / HOW IT IS IMPLEMENTED	IMPLEMENTATION STATUS	CONTROL OWNER
Organizational	A.5.22	Monitoring, review and change management of supplier services	Yes	Critical suppliers reviewed annually against SOC 2 / ISO 27001 evidence; performance and incidents tracked in the supplier register.	Implemented	
Organizational	A.5.23	Information security for use of cloud services	Yes	Cloud services onboarded through a documented assessment covering shared responsibility, data residency and exit.	Implemented	
Organizational	A.5.24	Information security incident management planning and preparation	Yes	Incident response plan defines severity levels, roles and escalation. Tested by tabletop exercise twice a year.	Implemented	
Organizational	A.5.25	Assessment and decision on information security events	Yes	Events triaged in Microsoft Sentinel against documented criteria; classification decisions recorded in the incident register.	Implemented	
Organizational	A.5.26	Response to information security incidents	Yes	Response procedures per incident class, with an evidence-preservation step before remediation.	Implemented	
Organizational	A.5.27	Learning from information security incidents	Yes	Post-incident reviews produce corrective actions tracked to closure; lessons feed the risk register and awareness content.	Implemented	
Organizational	A.5.28	Collection of evidence	Yes	Evidence handling procedure covers chain of custody and forensic imaging, with an external DFIR retainer for serious incidents.	Implemented	
Organizational	A.5.29	Information security during disruption	Yes	ICT continuity plan maintained alongside the BCP; RTO 4 hours and RPO 15 minutes for the production platform.	Implemented	
Organizational	A.5.30	ICT readiness for business continuity	Yes	ICT readiness validated by quarterly failover testing to the secondary Azure region; results recorded.	Implemented	
Organizational	A.5.31	Legal, statutory, regulatory and contractual requirements	Yes	Obligations register covers the Privacy Act 1988, the NDB scheme, APRA CPS 234 for regulated customers, and contractual commitments.	Implemented	
Organizational	A.5.32	Intellectual property rights	Yes	IP register maintained; open-source licence compliance enforced in CI through automated dependency scanning.	Implemented	
Organizational	A.5.33	Protection of records	Yes	Retention schedule applied through Purview retention labels; legal hold available and tested.	Implemented	
Organizational	A.5.34	Privacy and protection of PII	Yes	Privacy program aligned to the Australian Privacy Principles; PIAs required for any new processing of personal information.	Implemented	
Organizational	A.5.35	Independent review of information security	Yes	Independent review of the ISMS annually by an external assessor, plus the internal audit programme under clause 9.2.	Implemented	
Organizational	A.5.36	Compliance with policies, rules and standards for information security	Yes	Compliance monitored through quarterly control testing; exceptions raised as nonconformities with owners and due dates.	Implemented	
Organizational	A.5.37	Documented operating procedures	Yes	Operating procedures documented for all production systems and kept under version control alongside the code.	Implemented	
People	A.6.1	Screening	Yes	Background checks proportionate to role: identity and right-to-work for all hires, plus police check and referee checks for privileged and customer-data roles.	Implemented	
People	A.6.2	Terms and conditions of employment	Yes	Employment contracts include confidentiality, acceptable use and security obligations that survive termination.	Implemented	
People	A.6.3	Information security awareness, education and training	Yes	Security awareness at induction and annually, with simulated phishing every quarter and targeted follow-up training.	Implemented	
People	A.6.4	Disciplinary process	Yes	Disciplinary process for security breaches documented in the employee handbook and applied consistently.	Implemented	
People	A.6.5	Responsibilities after termination or change of employment	Yes	Post-employment obligations set out in the contract and restated in the exit letter.	Implemented	
People	A.6.6	Confidentiality or non-disclosure agreements	Yes	NDAs executed with all staff, contractors and suppliers before access is granted; reviewed when scope changes.	Implemented	
People	A.6.7	Remote working	Yes	Remote work policy mandates managed devices, full-disk encryption and no use of unmanaged personal equipment for customer data. Fully remote workforce makes this control central rather than peripheral.	Implemented	
People	A.6.8	Information security event reporting	Yes	Reporting channel via a dedicated Teams channel and security@ mailbox, with a no-blame policy stated explicitly to encourage reporting.	Implemented	

THEME	CONTROL	CONTROL NAME	APPLICABLE	JUSTIFICATION / HOW IT IS IMPLEMENTED	IMPLEMENTATION STATUS	CONTROL OWNER
Physical	A.7.1	Physical security perimeters	Yes	Applies to the Melbourne head office. Production infrastructure is Azure — physical security there is inherited from Microsoft and evidenced by their ISO 27001 and SOC 2 reports.	Implemented	
Physical	A.7.2	Physical entry	Yes	Office entry by swipe card with an access log; visitors escorted and signed in at reception.	Implemented	
Physical	A.7.3	Securing offices, rooms and facilities	Yes	Comms cabinet in the office is locked with access restricted to IT. Server rooms are not operated — no on-premises production infrastructure exists.	Implemented	
Physical	A.7.4	Physical security monitoring	Yes	Building-managed CCTV covers office entry points; footage retained 30 days by the building operator under the lease.	Implemented	
Physical	A.7.5	Protecting against physical and environmental threats	Yes	Environmental threats assessed for the office. Cloud regions selected in part on Microsoft's published environmental and resilience controls.	Implemented	
Physical	A.7.6	Working in secure areas	Yes	Clear-desk and clear-screen requirements apply in the office and to home workspaces where customer data is handled.	Implemented	
Physical	A.7.7	Clear desk and clear screen	Yes	Clear desk and clear screen enforced by policy and by a 5-minute automatic screen lock pushed through Intune.	Implemented	
Physical	A.7.8	Equipment siting and protection	Yes	Equipment siting covered by the office fit-out; screens positioned away from windows and walkways in client-facing areas.	Implemented	
Physical	A.7.9	Security of assets off-premises	Yes	Off-premises assets are laptops and mobiles, all Intune-enrolled, encrypted and remotely wipeable. This is the dominant case for a remote-first workforce.	Implemented	
Physical	A.7.10	Storage media	**No**	Excluded. Removable media is blocked at the endpoint by Intune device configuration; USB mass storage is disabled fleet-wide and no business process uses removable media. Exclusion is enforced technically, not by policy alone.	Not applicable	
Physical	A.7.11	Supporting utilities	Yes	Office power and network continuity provided under the lease. Production dependencies sit with Azure and are covered by the ICT continuity plan.	Implemented	
Physical	A.7.12	Cabling security	Yes	Office cabling secured within the building fabric and the locked comms cabinet.	Implemented	
Physical	A.7.13	Equipment maintenance	Yes	Endpoint maintenance handled through the managed device lifecycle; faulty devices are wiped before repair or disposal.	Implemented	
Physical	A.7.14	Secure disposal or re-use of equipment	Yes	Devices sanitised using certified erasure and disposed through an e-waste provider that issues destruction certificates, retained as evidence.	Implemented	
Technological	A.8.1	User endpoint devices	Yes	All endpoints Intune-managed with compliance policies gating access to corporate resources through Conditional Access.	Implemented	
Technological	A.8.2	Privileged access rights	Yes	Privileged access managed through Entra Privileged Identity Management with just-in-time elevation, approval and time limits.	Implemented	
Technological	A.8.3	Information access restriction	Yes	Access restricted by role at application and data layer; customer data access requires a logged business justification.	Implemented	
Technological	A.8.4	Access to source code	Yes	Source code access restricted by Azure DevOps project permissions; branch protection prevents direct commits to main.	Implemented	
Technological	A.8.5	Secure authentication	Yes	Phishing-resistant MFA and Conditional Access policies evaluate device compliance, location and risk on every authentication.	Implemented	
Technological	A.8.6	Capacity management	Yes	Capacity monitored through Azure Monitor with alerting thresholds; capacity reviewed monthly against growth forecasts.	Implemented	
Technological	A.8.7	Protection against malware	Yes	Microsoft Defender for Endpoint deployed fleet-wide with tamper protection enabled and alerts routed to Sentinel.	Implemented	
Technological	A.8.8	Management of technical vulnerabilities	Yes	Vulnerability management through Defender Vulnerability Management; remediation SLAs of 14 days for critical and 30 for high.	Implemented	
Technological	A.8.9	Configuration management	Yes	Configuration baselines defined in Intune and Azure Policy; drift detected and reported weekly.	Implemented	
Technological	A.8.10	Information deletion	Yes	Deletion governed by the retention schedule and Purview retention labels; customer data deleted within 30 days of contract end.	Implemented	
Technological	A.8.11	Data masking	Yes	Production data is never copied to non-production. Test environments use synthetically generated data.	Implemented	
Technological	A.8.12	Data leakage prevention	Yes	DLP policies in Purview cover customer data and personal information across Exchange, SharePoint, Teams and endpoints.	Implemented	
Technological	A.8.13	Information backup	Yes	Azure Backup with geo-redundant storage; restores tested quarterly and results recorded.	Implemented	

THEME	CONTROL	CONTROL NAME	APPLICABLE	JUSTIFICATION / HOW IT IS IMPLEMENTED	IMPLEMENTATION STATUS	CONTROL OWNER
Technological	A.8.14	Redundancy of information processing facilities	Yes	Production runs active-passive across two Azure regions; failover tested quarterly against the 4-hour RTO.	Implemented	
Technological	A.8.15	Logging	Yes	Logs centralised in Microsoft Sentinel with 12-month retention; log integrity protected by immutable storage.	Implemented	
Technological	A.8.16	Monitoring activities	Yes	Sentinel analytics rules generate alerts triaged by the security team; detection coverage mapped to MITRE ATT&CK.	Implemented	
Technological	A.8.17	Clock synchronisation	Yes	Time synchronised to Azure-provided NTP across all systems, ensuring log timestamps correlate.	Implemented	
Technological	A.8.18	Use of privileged utility programs	Yes	Privileged utilities restricted through PIM and application control; usage logged and reviewed monthly.	Implemented	
Technological	A.8.19	Installation of software on operational systems	Yes	Software installation controlled by Intune application allow-listing; users cannot install unapproved software.	Implemented	
Technological	A.8.20	Networks security	Yes	Network segmented into Azure virtual networks with network security groups; default-deny between tiers.	Implemented	
Technological	A.8.21	Security of network services	Yes	Service security requirements documented per service; private endpoints used for data-tier connectivity.	Implemented	
Technological	A.8.22	Segregation of networks	Yes	Production, staging and corporate networks are fully segregated with no lateral routes.	Implemented	
Technological	A.8.23	Web filtering	Yes	Web filtering through Defender for Endpoint network protection, blocking known-malicious and high-risk categories.	Implemented	
Technological	A.8.24	Use of cryptography	Yes	Cryptographic policy defines approved algorithms; TLS 1.2+ in transit, AES-256 at rest, keys in Azure Key Vault with rotation.	Implemented	
Technological	A.8.25	Secure development life cycle	Yes	Secure SDLC documented with threat modelling at design and security acceptance criteria before release.	Implemented	
Technological	A.8.26	Application security requirements	Yes	Security requirements captured as acceptance criteria on every user story touching authentication, authorisation or customer data.	Implemented	
Technological	A.8.27	Secure system architecture and engineering principles	Yes	Architecture principles documented, including zero-trust identity, least privilege and defence in depth.	Implemented	
Technological	A.8.28	Secure coding	Yes	Secure coding standards enforced through static analysis in CI; findings block the build at high severity.	Implemented	
Technological	A.8.29	Security testing in development and acceptance	Yes	Security testing in the pipeline (SAST, dependency scanning, secret detection) plus annual external penetration testing.	Implemented	
Technological	A.8.30	Outsourced development	No	Excluded. All development is performed in-house by employed engineers. No development is outsourced to third parties, so there is no outsourced development to control. Reassessed at each management review.	Not applicable	
Technological	A.8.31	Separation of development, test and production environments	Yes	Development, test and production are separate Azure subscriptions with no shared credentials or network paths.	Implemented	
Technological	A.8.32	Change management	Yes	Changes go through pull request, peer review and automated testing; production releases require change approval and have a documented rollback.	Implemented	
Technological	A.8.33	Test information	Yes	Test data is synthetic. Where production-like data is unavoidable it is masked before use and the masking is verified.	Implemented	
Technological	A.8.34	Protection of information systems during audit testing	Yes	Audit activities on production systems are scheduled, scoped in writing and performed read-only to avoid disruption.	Implemented	