InfraTrace360

InfraTrace360 — ISO/IEC 27001:2022 Control Coverage

How the InfraTrace360 application supports and provides evidence for Annex A controls. InfraTrace360 is a management & evidence tool — it helps you operate and demonstrate these controls; it does not by itself grant certification, which also requires policies, processes and people.

Annex A Control	Control Name	How InfraTrace360 supports it	Supporting module / feature
A.5.9	Inventory of information & associated assets	Maintain a live inventory of network assets and registered applications with owner, location and OS.	Asset Inventory; Applications
A.5.12	Classification of information	Classify documents as Public / Internal / Confidential / Restricted.	Document Inventory (Classification)
A.5.15	Access control	Record who has access to which application and role; enforce app-level role-based access internally.	Application Access; Roles
A.5.16	Identity management	Manage user identities and roles; optionally read identities live from Active Directory / LDAP.	Users & Roles; AD/LDAP
A.5.18	Access rights (provisioning & review)	Grant/track access rights and run per-person access reviews, exportable to PDF for sign-off.	Application Access; User Access Certification
A.5.19	Information security in supplier relationships	Maintain a supplier register with criticality and responsible department.	Vendors
A.5.22	Monitoring & review of supplier services	Record monitoring frequency and contract expiry; 'Expiring Soon' flags upcoming renewals.	Vendors; Expiring Soon
A.5.24	Incident management planning & preparation	Central incident register with type, severity, dates and status workflow.	Security Incidents
A.5.25	Assessment & decision on security events	Classify incidents by severity (Low→Critical) and occurrence (New/Recurring).	Security Incidents
A.5.26	Response to information security incidents	Capture action taken and drive status Open → In Progress → Closed.	Security Incidents
A.5.27	Learning from incidents	Retain description, action taken and closed date as a lessons-learned record.	Security Incidents; Audit Log
A.5.28	Collection of evidence	Attach supporting files (evidence) to any record across all modules.	Attachments (all modules)
A.5.37	Documented operating procedures	Register procedures/SOPs with version control and the document file attached.	Document Inventory
A.6.5	Responsibilities after termination/change	Track employment status (Resigned/Terminated) and verify access removal via access certification.	Employees; User Access Certification
A.8.2	Privileged access rights	Track service (non-human) accounts and local-admin exceptions with justification and expiry.	Service Accounts; Exceptions
A.8.3	Information access restriction	Role-per-application mapping and time-bound access exceptions with approval.	Application Access; Exceptions
A.8.15	Logging	Immutable-style audit log of every create/update/delete/import/export with before→after diffs, user & IP.	Audit Log
A.8.16	Monitoring activities	Review user activity and changes through the searchable, exportable audit log.	Audit Log
A.8.19	Installation of software on operational systems	Whitelist of approved software with approver and version control.	Approved Apps
Clause 6.1	Actions to address risks & opportunities	Full risk register: likelihood × impact scoring, auto priority, controls, response strategy, residual/target level.	Risk Register
Clause 8.2/8.3	Risk assessment & treatment	Score, prioritise and track treatment of risks with review dates and open actions.	Risk Register
A.5.10	Acceptable use & handling of assets	Register governance documents (acceptable-use, handling policies) with version and approval status.	Document Inventory
A.5.17	Authentication information	Password-hashed logins, role-based accounts and a login disclaimer for authorised-use acknowledgement.	Authentication; Settings
A.5.20	Addressing security within supplier agreements	Track supplier contracts, start/end dates and NDA-signed status.	Vendors (Contracts, NDA)
A.5.29	Continuity & readiness of ICT	Recurring compliance tasks/follow-ups and in-app backups support operational continuity.	Calendar; Backups
A.5.30	ICT readiness for business continuity	Automatic backups before updates and restore points.	Backups & In-App Updates
A.5.36	Compliance with policies & standards	Track policy documents and their approval status; monitor expiring obligations.	Document Inventory; Expiring Soon
A.6.1	Screening	Employee register provides the personnel record base that screening evidence attaches to.	Employees
A.6.2	Terms & conditions of employment	Hold employee records and attach signed terms; login disclaimer for acknowledgement.	Employees; Attachments
A.6.6	Confidentiality / non-disclosure agreements	Record NDA-signed status for suppliers/guests; attach the signed NDA.	Vendors; Guests; Attachments
A.8.8	Management of technical vulnerabilities	Log vulnerabilities/weaknesses as incidents and track them to closure in the risk register.	Security Incidents; Risk Register
A.8.9	Configuration management	Maintain an approved-software baseline with versions and least-privilege notes.	Approved Apps
Clause 9.1	Monitoring, measurement & evaluation	Dashboards, expiring-item alerts and audit log provide ongoing measurement and evidence.	Dashboard; Expiring Soon; Audit Log