

Template 3: control mapping and gap analysis

Each ISO/IEC 27090 mitigation theme mapped to the ISO/IEC 27002:2022 control already operated. Yellow cells are inputs.

#	ISO/IEC 27090 mitigation theme	ISO/IEC 27002:2022 control(s)	Applies to systems	Status	Evidence	Action	Owner	Due	Priority	Notes
1	AI asset inventory	5.9 Inventory of information and other associated assets	All	In place	Template 1 register maintained by CIO office	Add vendor SaaS AI features	CIO office	2026-11-30	Low	
2	Threat identification and risk assessment	5.7 Threat intelligence; ISO/IEC 27001 clause 6	All	Partial	Template 2 completed for AI-001 only	Complete Template 2 for all high-tier systems	Security lead	2026-12-31	Medium	
3	Supplier, model and data assurance	5.19, 5.20, 5.21 Supplier relationships and ICT supply chain	AI-001, AI-003	Partial	Vendor questionnaire on file	AI bill of materials; signed artefacts; contract clauses for logging	Procurement	2027-03-31	Medium	
4	Logging of prompts, outputs, versions and tool calls	8.15 Logging; 8.16 Monitoring activities	AI-001, AI-002, AI-003	Partial	Platform logs exist; no template versioning	Add model and template version fields; retention policy	Security lead	2027-01-31	Medium	
5	Secure development environment	8.25 Secure development life cycle; 8.31 Separation of environments; 8.4 Access to source code	AI-001	In place	Environment separation review 2026	Extend to notebooks, checkpoints and retrieval stores	Head of engineering	2027-03-31	Low	
6	Architecture, authentication and rate limiting	8.27 Secure system architecture; 8.5 Secure authentication; 8.20 Network security	AI-003	Missing	None	Configure per-client quotas; round confidence scores	Platform team	2027-01-31	High	
7	Adversarial testing and red teaming	8.29 Security testing in development and acceptance; 8.8 Technical vulnerabilities	All high tier	Missing	None	Engage tester; annual exercise including indirect prompt injection	Security lead	2027-03-31	High	
8	Treat model output as untrusted in integrations	8.25 Secure development life cycle; 8.28 Secure coding	AI-002, AI-003	Partial	Web output encoded; agent tool permissions unreviewed	Review tool permissions; add human approval step for risky actions	Head of engineering	2027-01-31	Medium	
9	Data provenance and integrity for training and retrieval data	5.12 Classification; 8.9 Configuration management; 5.33 Protection of records	AI-001, AI-002	Missing	None	Provenance checks and data snapshots before each retraining	Data owner	2027-03-31	High	
10	Monitoring for drift and decay; revalidation after change	8.16 Monitoring activities; 8.32 Change management	All	Missing	None	Define thresholds; revalidation gate in change management	Platform team	2027-03-31	High	
11	Combined (holistic) evaluation of controls before deployment	8.29 Security testing in development and acceptance	All high tier	Missing	None	Add combined-control test to acceptance criteria	Security lead	2027-03-31	High	
12	AI incident response playbooks	5.24 to 5.28 Incident management planning and response	All	Missing	None	Three playbooks (poisoning, leakage, injection-driven action); tabletop exercise	Security lead	2027-03-31	High	
13	AI security policy and roles	5.1 Policies for information security; 5.2 Roles and responsibilities	All	Partial	Draft policy (Template 4)	Approve policy; publish RACI	CIO	2026-12-31	Medium	
14	Awareness for developers and users of AI	6.3 Information security awareness, education and training	All	Missing	None	Briefing for developers on prompt injection and output handling	Security lead	2027-03-31	High	

Summary

Themes assessed	14
In place	2
Partial	5
Missing	7
Not applicable	0
Coverage (in place / applicable)	14%

How to use this sheet

Yellow cells are inputs. All rows shown are example values in blue italics taken from the course; overwrite them with the real position.

Status drop-down: In place, Partial, Missing, Not applicable. Priority calculates from Status (Missing = High, Partial = Medium).

Keep a link or file reference in Evidence so audits do not restart from zero. Control names are listed on the 27002 reference sheet.

Template by Shahzad Asghar, CISSP, CISM. Free ISO/IEC 27090 course and templates: shahzadasghar.com/learn/iso-27090/templates. Licensed CC BY 4.0: reuse and adapt with attribution.

ISO/IEC 27002:2022 controls referenced

Control titles as published in ISO/IEC 27002:2022.

Control	Title
5.1	Policies for information security
5.2	Information security roles and responsibilities
5.7	Threat intelligence
5.9	Inventory of information and other associated assets
5.12	Classification of information
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
5.24	Information security incident management planning and preparation
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.33	Protection of records
6.3	Information security awareness, education and training
8.4	Access to source code
8.5	Secure authentication
8.8	Management of technical vulnerabilities
8.9	Configuration management
8.15	Logging
8.16	Monitoring activities
8.20	Networks security
8.25	Secure development life cycle
8.27	Secure system architecture and engineering principles

8.28	Secure coding
8.29	Security testing in development and acceptance
8.31	Separation of development, test and production environments
8.32	Change management