

First AI threat assessment workshop

Agenda, participants, pre-reads and invitation text. Proposed date: Tuesday 3 November 2026, 09:00 to 12:00 (adjust in the .ics file if needed).

Objective

Complete the ISO/IEC 27090 threat and risk assessment (Template 2) for AI-001, the recruitment screening model, as the first High-tier system, and agree the method the team will reuse for the other systems.

Outputs

- Completed Template 2 workbook for AI-001 with scores, gaps and treatment owners.
- Agreed scoring scale and treatment thresholds for the organisation.
- First entries in Template 3 (control mapping) based on the gaps found.
- Date and system for the second workshop.

Participants

Role	Name	Why needed
Security lead (facilitator)	[name]	Owns the assessment and the threat catalogue
Business owner, AI-001	[name]	Impact scoring, acceptance decisions
Technical owner, AI-001	[name]	Architecture, integrations, logging reality
Data owner, AI-001	[name]	Training and fine-tuning data provenance
Vendor contact (optional, part 2 only)	[name]	Supplied model assurance, artefact signing
Legal / privacy	[name]	Personal data, regulatory exposure
CIO office representative	[name]	Inventory, budget, roadmap link

Pre-reads (send with the invitation)

- Course lessons 5 to 8 (threat catalogue) and lesson 10 (templates) at shahzadasghar.com/learn/iso-27090.
- Template 2 workbook, Threat catalogue and Scales sheets.
- Inventory record for AI-001 and the vendor's model documentation.
- Latest architecture diagram and data flow for AI-001.

Agenda (3 hours)

Time	Item	Lead	Output
09:00	Purpose, ground rules, how scoring works (Scales sheet)	Facilitator	Shared understanding
09:15	Walk through AI-001: data flow, model source, exposure, users	Technical owner	Assets and entry points on the board
09:45	Threats 1 to 6: poisoning, evasion, membership inference, inversion, exfiltration, direct model poisoning	Facilitator	Likelihood, impact, existing controls per threat
10:30	Break		

Time	Item	Lead	Output
10:40	Threats 7 to 9 and Annex B: sensitive output, prompt injection, output injection, theft and leakage	Facilitator	Scores and gaps
11:15	Treatments: owner, due date, link to Template 3	Business owner	Treatment plan
11:45	Review summary, residual risk statement, next workshop	Facilitator	Decisions recorded
12:00	Close		

Logistics

- Location: [room or video link]
- Materials: Template 2 workbook open on screen; whiteboard; printed threat catalogue.
- Recorder: [name] keeps the workbook updated live.

Invitation text (copy into the calendar invite)

Subject: AI threat assessment workshop, AI-001 recruitment screening model (ISO/IEC 27090)

Following the adoption of ISO/IEC 27090:2026 as our reference for AI security, we are holding the first AI threat assessment workshop. We will score the twelve threats in the standard against the recruitment screening model, identify gaps and assign treatments. Please read the threat catalogue summary and Template 2 before the session, and bring the current architecture and data flow for the system.

Date: Tuesday 3 November 2026, 09:00 to 12:00. Location: [room or video link]. Facilitator: [security lead].

Attachments: threat catalogue summary, Template 2 workbook, inventory record for AI-001.

A calendar file (iso-27090-threat-assessment-workshop-invite.ics) is provided alongside this document.