KORUR

AI SECURITY TRAINING · RISK ASSESSMENT

AI Risk Assessment Template

A starter framework for assessing the security and compliance risk of AI tools across your organization.

Your team is already using AI. The question is whether they're doing it safely, and whether you know about all of it.

Why AI Security Is Non-Optional in 2026

AI adoption outpaced AI governance by years. The security debt is now coming due.

65%

Shadow AI Is Everywhere

65% of employees use AI tools at work, most without any company policy, DPA assessment, or security review of the tools involved.

10x

AI Phishing Is Indistinguishable

AI-generated spear-phishing is 10x more convincing than traditional templates, perfect grammar, accurate personal context, and no obvious red flags.

AI Act

EU AI Act Compliance Obligations

The EU AI Act creates compliance obligations for organizations deploying or using AI systems. Training records and governance policies are expected.

GDPR

GDPR Risk From AI Tool Usage

Data sent to AI providers may constitute an unlawful international transfer or a GDPR Article 28 violation without a proper Data Processing Agreement in place.

What Your Team Walks Away With

Practical governance, detection skills, and configuration knowledge your team applies immediately.

- A ready-to-deploy AI Acceptable Use Policy template tailored to your organization
- Ability to recognize AI-generated phishing, deepfake voice calls, and synthetic social engineering
- A GDPR-compliant AI tool inventory identifying which tools require DPA review
- Configuration knowledge for Microsoft Copilot, ChatGPT Enterprise, and Google Workspace AI data controls
- Prompt injection awareness: how attackers exploit AI-connected workflows and what to watch for
- A governance framework for approving, auditing, and revoking AI tool access across your organization

Assessment & Training Program

One focused day that transforms how your team thinks about AI tools.

1. **AI Threat Landscape**

   We start with the actual risks: shadow AI data exposure, prompt injection attacks, AI-generated phishing, and credential theft via AI tools.

2. **Shadow AI Discovery Exercise**

   Participants audit their own tool usage and map the data flows, what's going to AI providers, under what terms, and what the exposure looks like.

3. **AI Phishing Recognition Lab**

   Hands-on: participants work through real AI-generated phishing samples, learn the new detection heuristics, and practice reporting workflows.

4. **Configuration and Controls**

   Role-specific breakouts: IT teams configure data controls in Copilot/ChatGPT Enterprise; general staff practice the AI Acceptable Use Policy.

5. **Governance Workshop**

   We close with a collaborative session to build or review your AI governance framework, approval process, audit trail, incident escalation for AI-related events.

This document is a companion to Korur's AI Risk Assessment Template. It summarizes the framework covered during the live training. The hands-on labs, role-specific breakouts, and Q&A take place during the session itself.

Ready to run this with your team?
Korur delivers this training on-site, tailored to your industry and stack. Book a session at **korur.nl/contact**.