Risk-Management Register and Controls Map — Anonymised Sample

Risk-Management Register and Controls Map — Anonymised Sample

> **Anonymised — Do not redistribute.** Excerpt from a Documentation Sprint deliverable. The customer "Acme Decisions Ltd" and the AI system "AcmeMatch" are illustrative.

Customer: Acme Decisions Ltd · **AI System:** AcmeMatch v3.4 (high-risk, Annex III §4(a)) · **Register version:** 1.0 · **Last review:** 2026-04-25

Purpose

This register satisfies **EU AI Act Article 9** (Risk-management system for high-risk AI systems). It identifies, evaluates, and assigns controls to known and reasonably foreseeable risks across the lifecycle of AcmeMatch.

The register is paired with the **controls map** in §3 below, which links each risk to one or more controls, an owner, and a verification method.

This sample shows **6 representative risks of the 18** in the full register. The full register includes additional risks across data-governance, cybersecurity, and post-market monitoring categories.

1. Risk register (sample rows)

ID	Risk	Source / category	Likelihood (1-5)	Impact (1-5)	Inherent risk	Mitigations applied	Residual risk	Owner	Last review
R-01	Recruiter over-relies on AcmeMatch ranking and skips human review ("automation bias")	Article 14 — Human oversight	4	4	16 (High)	CTRL-001, CTRL-002, CTRL-003, CTRL-007	6 (Low-Med)	Head of Product	2026-0
R-04	Indirect demographic proxy bias in ranking output (e.g. CV-language correlations)	Article 10 — Data governance + Article 15 — Fairness	4	5	20 (Critical)	CTRL-004, CTRL-005, CTRL-006	8 (Med)	Head of ML	2026-0
R-07	Training data drift over time degrades ranking quality	Article 15 — Robustness	3	3	9 (Med)	CTRL-008, CTRL-009	4 (Low)	Head of ML	2026-0
R-09	Adversarial CV crafted to game the ranker (data poisoning at inference)	Article 15 — Cybersecurity	3	3	9 (Med)	CTRL-010, CTRL-011	4 (Low)	Head of Security	2026-0
R-12	Personal data of candidates retained beyond purpose-limitation period	UK GDPR Art. 5(1)(e) + AI Act Art. 12 logging	3	4	12 (High)	CTRL-012, CTRL-013	4 (Low)	DPO	2026-0
R-15	Post-market issue not detected because no Deployer	Article 72 — Post-market monitoring	3	4	12 (High)	CTRL-014, CTRL-015	6 (Low-Med)	Head of Product	2026-0

ID	Risk	Source / category	Likelihood (1-5)	Impact (1-5)	Inherent risk	Mitigations applied	Residual risk	Owner	Last review
	feedback loop								

(Inherent and residual risk are likelihood × impact on a 5×5 matrix. Cells marked Critical (≥ 16) trigger mandatory weekly review until reduced.)

---

2. Risk treatment notes (per representative row)

R-01 — Automation bias

- **Why it matters:** the AI Act's high-risk regime presumes the human-in-the-loop is *meaningful*, not nominal. Rubber-stamping a ranking is the most-cited regulatory failure mode for hiring AI.
- **Treatment:** UI design forces the recruiter to interact with each candidate's rationale before moving them to the next stage; the "explain this rank" link logs an oversight event; recruiters who consistently skip override actions are flagged for retraining via CTRL-007.

R-04 — Indirect demographic proxy bias

- **Why it matters:** even with explicit demographic features stripped, language patterns in CVs correlate with demographic groups (e.g. educational institution, language register, gendered hobbies). This is the highest-impact, hardest-to-detect risk in employment AI.
- **Treatment:** quarterly bias audit on the held-out evaluation set with sub-group parity metrics (selection rate parity, top-N recall parity) reported back to the Provider. Any sub-group with > 0.05 deviation triggers a model-card review and possible retraining.

R-07 — Training data drift

- **Treatment:** monitor input embedding PSI per role family; retrain when PSI > 0.15 sustained over 30 days.

R-09 — Adversarial CV / data poisoning

- **Treatment:** input sanitisation, file-type strict whitelist, length and entropy bounds, output anomaly detection (sudden rank distribution shifts trigger an automatic review).

R-12 — Personal data over-retention

- **Treatment:** automated deletion 30 days after the recruiter closes the role unless explicit candidate consent is captured for talent pool retention.

R-15 — Post-market blind spot

- **Treatment:** in-product "report a problem" flow that creates a structured incident in the Provider's incident workflow per Article 73, monthly Deployer health-check call, and quarterly post-market monitoring report aligned to Article 72.

---

3. Controls map (sample)

Control ID	Control	Linked risks	Implementation status	Verification method	Verification frequency	Owner
CTRL-001	"Override and re-rank" UI control on every shortlist	R-01	Live in v3.4.0	UI behaviour test + log inspection	Per release	Head of Product
CTRL-002	Per-candidate "explain this rank" link, mandatory before "move to interview"	R-01	Live in v3.4.0	UI behaviour test + log inspection	Per release	Head of Product
CTRL-003	Recruiter activity log captures every override / skip event for audit	R-01	Live	Log retention review	Quarterly	Head of Product
CTRL-004	Demographic-feature stripping at ingestion (name, age, gender, nationality)	R-04	Live	Code review + ingestion replay test	Per release	Head of ML
CTRL-005	Quarterly bias audit on held-out evaluation set, sub-group parity metrics	R-04	Q1 done; Q2 outstanding	Audit report archived to Annex IV §3.3	Quarterly	Head of ML
CTRL-006	Bias-audit deviation > 0.05 triggers model-card review and possible retrain	R-04	Process drafted; not yet exercised	Procedure walkthrough	Annually	Head of ML
CTRL-007	Recruiter consistency-check: alert if override rate < 5% over 50 shortlists	R-01	Live	Weekly anomaly report	Weekly	Head of Product
CTRL-008	PSI monitoring on input embedding distributions per role family	R-07	Live	Dashboard + alert at PSI > 0.15	Daily	Head of ML
CTRL-009	Retraining playbook with rollback to last-	R-07	Drafted	Tabletop exercise	Annually	Head of ML

Control ID	Control	Linked risks	Implementation status	Verification method	Verification frequency	Owner
	known-good model weights					
CTRL-010	Input sanitisation, file-type whitelist, size and entropy bounds	R-09	Live	Penetration test report	Annually	Head of Security
CTRL-011	Output anomaly detection on rank distribution per role family	R-09	Live	Alert review log	Monthly	Head of Security
CTRL-012	Automated deletion of candidate data 30 days after role close (default)	R-12	Live	Deletion job log review	Monthly	DPO
CTRL-013	Talent-pool retention requires explicit candidate consent capture	R-12	Live	Consent record review	Quarterly	DPO
CTRL-014	"Report a problem" flow generates structured incident under Article 73	R-15	Live	Incident log review	Monthly	Head of Product
CTRL-015	Monthly Deployer health-check call + quarterly post-market monitoring report	R-15	Live	Report archive	Quarterly	Head of Product

4. How this register is used

1. **At Provider's monthly governance review:** every Critical (≥ 16) inherent risk is reviewed regardless of residual; one randomly selected High row and one randomly selected Medium row are also reviewed.
2. **At a notified body / market surveillance request:** this register, the linked controls map, the Annex IV technical documentation, and the post-market monitoring report constitute the response pack.
3. **At a Deployer procurement questionnaire response:** sample rows are extracted for the supplier questionnaire response pack (see `06-supplier-questionnaire-response-sample.md`).
4. **At each material model change:** all rows where the risk is materially affected by the change are re-scored and the residual risk is recomputed before the change is released.

Document control

Item	Detail
Sample produced	2026-04-25
Anonymised customer	Acme Decisions Ltd (fictional UK SME)
AI system in scope	AcmeMatch v3.4
Tier of artefact	Documentation Sprint (full register populates 18 rows; sample shows 6)
Reviewer	Customer's solicitor, DPO, or risk lead before external reliance

---

Prepared with support from GeraCompliance. This document is not legal advice and does not guarantee compliance. The customer remains responsible for legal review, implementation, and regulatory obligations.