🧮 AI Updates for Organization's Enterprise Risk Register

☀️ Sandy Dunn

Define AI/GenAI as a Distinct Risk Category

- ☐ Add **AI/GenAI Risk** as a formal category in your enterprise risk taxonomy alongside traditional ones like Cybersecurity, Legal/Compliance, Operational, Strategic, Reputational.
- ☐ GenAI introduces novel risks (e.g., prompt injection, model drift, hallucination) that are distinct from traditional IT/cyber risks.

Standardize the Risk Statements for GenAI

Each entry in the risk register should have clear, actionable language.

Examples:

- ☐ Risk of sensitive information disclosure via GenAI outputs (e.g., inadvertent data leakage through LLMs).
- ☐ Risk of reputational damage due to GenAI-generated misinformation or bias in outputs.
- ☐ Risk of unauthorized model manipulation via prompt injection leading to operational disruption.
- ☐ Risk of regulatory non-compliance due to unmonitored GenAI decision-making.

Link GenAI Risks to Enterprise Objectives

Tie each GenAI risk to broader business objectives or value stream:

- ☐ Operational continuity
- ☐ Brand and customer trust
- ☐ Regulatory compliance
- ☐ Data protection

Assign Clear Risk Owners

- ☐ Who has decision making authority? Often it's a combination: the CISO (for security risks), CIO (for operational risks), General Counsel (for compliance risks), and in larger organizations the Chief AI Officer.
- ☐ Make it explicit! Who monitors and mitigates GenAI risks so it doesn't fall between cyber and business teams?

Use Risk Assessment Criteria Consistently

Apply the organization's enterprise risk matrix to GenAI risks:

- ☐ **Impact**: How severe is the worst-case scenario? (financial loss, legal fines, reputational damage)
- ☐ **Likelihood**: How likely is this risk given the GenAI systems deployed?
- ☐ **Velocity**: How fast could the risk materialize once triggered? (AI risks often have high velocity e.g., a hallucinated financial statement can cause immediate media attention.

Integrate Incident Data for Monitoring and Reassessment

- ☐ After any GenAI incident, feed the root cause analysis and lessons learned back into the risk register.
- ☐ Adjust risk likelihood or impact based on trends:
  - ☐ Are prompt injection attempts increasing?
  - ☐ Are hallucinations causing more escalations?

Connect to Mitigation and Controls

Document the **controls** for each GenAI risk:

- ☐ Red teaming GenAI apps
- ☐ Prompt hardening
- ☐ Model output monitoring
- ☐ Human-in-the-loop (HITL) review processes
- ☐ Data governance for training datasets

Reporting and Executive Dashboards

- ☐ Include GenAI risks in regular risk committee or board risk dashboard reports.
- ☐ Highlight emerging risks or regulatory updates related to AI (e.g., EU AI Act, U.S. AI Executive Orders).
- ☐ Use heatmaps or radar charts showing where GenAI risks sit relative to other enterprise risks.

Example GenAI Risk Register Entry

Risk ID	Risk Description	Impact	Likelihood	Velocity	Owner	Controls	Status
AI-001	Unauthorized prompt injection could cause	High	Medium	High	CISO / Chief AI Officer	Prompt validation, API gating,	Open mitigation in progress

	GenAI to leak sensitive data.					model monitoring	
AI-002	Bias in GenAI outputs may result in reputational harm or lawsuits.	High	Low	Medium	Chief Risk Officer / Legal	Output audits, bias testing, incident response plan	Mitigated