Session 1 Handout: What Governance Means in a Small Company

FAST-10 AI Governance, Risk, Ethics, and Responsible Use · 7formations · Instructor: Wadood Chaudhary · All examples fictional · Training, not legal advice

> **Training, not legal advice.** Confirm your employer's obligations with its counsel or compliance lead.

Why this session matters

Your staff are already using AI, approved or not, and AI features are switching on inside software you already pay for. Customers, insurers, and owners increasingly ask, "How do you control it?" Governance in a 40-person company is not a committee and a binder. It is one owner, an inventory, a short policy, and checks matched to risk.

Key concepts

1. Right-sized governance

- A few clear rules, named owners, and checks.
- **Match controls to risk, not company size.** A 15-person dental practice using a patient chatbot has high-risk AI; a 200-person firm using AI for meeting agendas may not.
- Start with: owner → inventory → policy → register → incident plan.

2. NIST AI RMF in plain terms

Function	Plain meaning	Small-company example
Govern	Roles, policy, accountability, culture	Name an owner; approve the AUP; train staff
Map	Where AI is used, for whom, what could go wrong	The inventory; context for each use
Measure	Test and track the risks	Test script; monthly sample review
Manage	Act on risks and incidents	Turn off a feature; run the incident checklist

The AI RMF 1.0 (January 2023) is **voluntary**; use the parts that fit. The Generative AI Profile (NIST AI 600-1, July 2024) lists 12 generative-AI risks, including confabulation, data privacy, harmful bias, and information security. As of October 2026 NIST has signaled revisions and is developing additional profiles; check the NIST page for the current version.

3. Other frameworks you will hear about

Framework	What it is	When it matters to an SME
ISO/IEC 42001:2023	Certifiable AI management-system standard (plan-do-check-act)	When a large customer or partner asks for certification or alignment

Framework	What it is	When it matters to an SME
EU AI Act	EU regulation with risk tiers; reaches providers and deployers outside the EU	When you sell AI-enabled products or services into the EU, or your AI output is used there
OWASP Top 10 for LLM Applications (2026)	Security risks for LLM apps	When you deploy chatbots, agents, or AI connected to your systems

4. The inventory: sanctioned and shadow AI

Find AI in three places: **approved tools**, **built-in features** in existing software (CRM, ERP, HR, meetings), and **shadow use** (staff using tools on their own). Use an anonymous survey and an amnesty: you want honest answers, not hidden use.

Each row: tool or use · type · what it does · data touched · owner · risk · next action. **No inventory, no governance.**

Worked example (fictional)

Bayside Precision Parts found 13 inventory rows, not the 1 they expected: 5 built-in features (including an HR résumé-match tool someone had switched on), 5 shadow uses, and a gap for 33 staff who didn't answer. The three high-risk rows (résumé match, an estimator uploading customer drawings to a free image tool, supervisors' AI note-taker) got immediate actions that week.

Checklist

- ☐ Governance owner named.
- ☐ Inventory includes built-in features and shadow use.
- ☐ Each row has data touched, an owner, and a next action.
- ☐ High-risk rows have action dates.
- ☐ Repeat schedule set (for example, twice a year and at each new tool).

Do and don't

Do	Don't
Offer amnesty for disclosing shadow AI	Punish people for honest survey answers
Check release notes for new AI features	Assume "we didn't buy AI" means "we don't use AI"
Match controls to risk	Copy a bank's policy wholesale
Use the frameworks as menus	Try to implement every NIST subcategory