



COMPLIANCE AS A **COMPETITIVE ADVANTAGE**

AI Governance · Data Protection · Responsible Adoption

Interactive Roundtable Workshop | 45 Minutes



GOVERN

PROTECT

ENABLE

HOW THIS SESSION WORKS

50 minutes · 5 segments · you do most of the talking

01

8 min

Opening + Shadow AI Reality Check

One question. Real examples. Sets the stakes.

02

10 min

Where Are You? (Pulse Check)

Live poll + table discussion. Find your posture.

03

17 min

Three Locks + Three Activities

Framework intro, then you apply it at your table.

04

10 min

Real-World Scenario Breakout

Your table picks a scenario and works all three locks.

05

5 min

Your 30-Day Sprint

Individual. Posture-matched. Written down before you leave.



"Raise your hand if your team has used an AI tool in the last 30 days that your IT or compliance team doesn't officially know about."

That's not a compliance failure. That's a signal. Your people are hungry to move faster. Today we figure out how to build the road, not just the guardrails.

TURN TO YOUR TABLE →

What AI tools is your team currently using — officially or not?
Go around once, 30 seconds each.

🕒 2 minutes — no judgment zone



THE SHADOW AI REALITY CHECK

None of these people thought they were doing anything wrong.



The Contract Summary

An employee pastes a client contract into ChatGPT for a plain-English summary.

The contract contains PII, commercial terms, and confidential IP.

Data Exfiltration Risk



The AI Note-Taker

A manager uses an AI transcription tool on a video call with a patient.

The tool stores recordings on overseas servers with unknown retention policies.

Regulatory Compliance Risk



The Excel Spreadsheet

Finance uploads a quarterly P&L to an AI analytics tool to find anomalies faster.

The tool's terms allow training on uploaded content.







IP & Financial Data Risk



Gartner: By 2027, more than 40% of AI-related data breaches will be caused by improper use of generative AI — not external attacks.

THE GOVERNANCE GAP







WHERE AI IS HAPPENING

-  Email drafting tools
-  AI note-takers in meetings
-  ChatGPT for research
-  AI analytics platforms
-  Copilot / embedded AI in SaaS
-  Image & content generators



**Your
Risk
Surface**

WHERE GOVERNANCE EXISTS

-  General IT acceptable use
-  Outdated data policy
-  AI-specific policy
-  Vendor risk process for AI
-  Data classification system
-  Shadow AI monitoring

ASK YOURSELF RIGHT NOW:

- ① Do you know every AI tool being used in your org today?
- ② Do you know what data has touched those tools?
- ③ Do you have a process for evaluating new AI tools before adoption?

THE THREE LOCKS FRAMEWORK

Every lock you close opens a door.

LOCK 1 • GOVERN



*You can't govern
what you can't see*

Visibility is the foundation. Discover every AI tool in use across your organization — approved or not.

LOCK 2 • PROTECT



*Data sovereignty
is your superpower*

Once you see clearly, protect what matters. Build controls around your data, your vendors, and your people.

LOCK 3 • ENABLE



*Confident adoption,
not fearful avoidance*

Governance unlocks speed. Give your teams approved tools, clear guidance, and the confidence to move fast.

GOVERN → PROTECT → ENABLE | Each step builds on the last. You can start anywhere — but you cannot skip steps.

GOVERN

"You can't govern what you can't see"



AI & 365 INVENTORY AUDIT

Know what's in the building

- › Approved tools (IT-sanctioned)
- › Unapproved / Shadow AI tools
- › Embedded AI in existing SaaS
- › MS 365 Audit / Access & Permission reviews

💡 Most orgs find 3–5× more tools than IT expects



THE ONE-PAGE AI POLICY

Not a 40-page document nobody reads

- › 5 core rules, plain language
- › Living document — updated quarterly
- › Signed off by leadership

💡 Template in your resource pack



USE CASE RISK TIERING

Classify AI use by risk level

- › ● Low: summarising public info
- › ● Medium: internal data analysis
- › ● High: client data, regulated info
- › ● Critical: autonomous decisions

💡 Tiering template in resource pack

PROTECT

"Data sovereignty is your superpower"



DOES IT TRAIN ON YOUR DATA?

The question every employee should ask

✗ **Training ON your data:**

Content improves their model

✓ **NOT training on your data:**

Your input stays private

💡 This one question eliminates ~60% of your AI data risk



DATA CLASSIFICATION BASICS

If your people can't see it, they can't protect it

📘 **Public**

📁 **Internal**

🔒 **Confidential**

🚫 **Restricted / Regulated**

💡 Labels must be visible, not buried in policy docs



VENDOR DUE DILIGENCE

5 questions before you sign

1. Does it train on our data?
2. Where is data stored? Jurisdiction?
3. What is your data retention policy?
4. SOC 2 / ISO 27001 certified?

💡 Full 10-question checklist in your resource pack



THE SAFE SANDBOX MODEL

A low-risk environment to experiment

- › Isolated test environment
- › Non-production / demo data
- › Defined scope & time limits
- › Fast feedback loop to IT / security

💡 This kills Shadow AI — if there's a safe place to try things, people use it



AI CHAMPIONS PROGRAMME

Guides, not gatekeepers

- › 1 per department minimum
 - › Monthly sync with IT / security
 - › First to test new tools
 - › Trusted voice with their peers
- 💡 Cost: almost zero. Impact: enormous



THE GREEN LANE

Pre-approved AI tool list

- › Tool name & approved use cases
 - › What data can / can't be used
 - › Who to contact for access
 - › Review date (quarterly)
- 💡 Evaluation Scorecard in your resource pack

YOUR ORG, RIGHT NOW

Small Group Discussion | 12 Minutes | Use the card on your table

CARD A

THE GOVERNANCE GROUP

"What would your AI policy say if you wrote it this afternoon? What are your 3 non-negotiables?"



CARD B

THE RISK GROUP

"Walk through your most sensitive data type. Trace the path it could take if an employee used an unauthorised AI tool today."



CARD C

THE OPPORTUNITY GROUP

"If you had a compliance-approved AI toolkit tomorrow — what's the first use case you'd launch? What would it be worth?"



 12 minutes → each group shares ONE key insight

THE 30-DAY SPRINT

Don't leave with good intentions. Leave with a next step.

IF YOU'RE STARTING



Conduct full AI tool inventory



Identify 1 high-risk use case



Draft 5-rule AI use policy



Find your shadow AI exposure



Brief leadership on the gap

IF YOU HAVE A FOUNDATION



Publish your AI policy (v1)



Complete top vendor audits



Create your 'Green Lane' list



Run data classification audit



Set up Copilot governance review

IF YOU'RE SCALING



Launch AI Champions programme



Build continuous monitoring



Pursue AI-specific certification



Develop AI risk register



Quarterly AI governance review

"The organizations that win in regulated industries aren't those who waited until AI was perfectly safe. They're the ones who built the infrastructure to adopt it responsibly while others were still debating."

DEMO

Need help on your AI journey?

We offer AI Consulting:

- AI Assessments
- Training & Adoption
- Champions Program
- Governance & Compliance
- AI Scaling from users > departments & org-wide
- AI Use-case identification & development (crawl, walk, run approach)
 - Prompt engineering & prompt libraries
 - Workflow & AI Agent consulting



YOUR RESOURCE PACK



Everything from today — and more — to take back and use on Monday.



AI Risk Tiering Template

4-tier classification system with approval requirements



Vendor Security Checklist

10-question due diligence tool for every AI vendor



Green Lane Scorecard

12-point evaluation system with approval thresholds



5-Rule Policy Template

Ready-to-edit AI use policy for your organization



30-Day Sprint Card

Tear-off action card with owner & timing columns



Full Resource Pack



Questions? · Scan the QR for digital resources · Thank you for the conversation today