

AI Risk Controls

The control stage of the Risk Spine: turn a sized tier into the controls that hold it.

POV

Put controls at the layer the risk lives on, not everywhere. A tier label is not a plan; controls are.

THE MODEL DEVICE · THE CONTROLS FLOOR — THE UNION OF FOUR LAYERS, SIZED TO ONE USE CASE

BASELINE · 10

FROM THE GATE

The legal + tripwire floor under every use case.

AXIS MODIFIER · 12

FROM THE RADAR

Targeted controls per axis: Agency · Reach · Data · Governability.

TIER DELTA · 9

FROM THE TIER

Stacks as the tier climbs S to XL: inherit-and-add.

GPAI OVERLAY · 4

FROM THE GPAI FLAG

Provider-side duties you evidence and inherit, not own.

FRAME · WHAT IT DOES

- Selects proportionate controls by layer for a sized use case, with named owners and evidence.
- When to run: after M10 risk sizing, once a tiered use case needs its control set defined.
- Inputs: M10 tier, lit Radar axes, GPAI flag; existing baseline; platform + ownership map.

WORK · IN THE ROOM

- The four layers and the colour contract; FIRM vs FLEX; the seven-field control object.
- Worked example (Wyreld) and the operating cadence; five calibration moves; 90-day playbook.
- Format: ~90-min to half-day facilitated workshop. Overview, teach, co-design, outcomes.

VALUE · WHAT YOU LEAVE WITH

- A proportionate control set per tier, each control named, owned, evidenced and on a cadence.
- Populated T11 Catalogue; O11 capture of selections, decisions and actions.
- Exit: controls selected and owned, ready for M12 Living Governance and M13 Evidence.

CO-DESIGN CANVAS SET · THREE STANDALONE ONE-PAGERS, EACH CIRCULATE-ABLE

1 · CONTROLS FLOOR CANVAS

One per use case: which controls land at each layer, with owner, evidence, cadence.

SO WHAT · THREE ROLES

Enterprise Architect · Transformation Leader · Microsoft Partner

2 · CONTROL-DEFINITION CARD

One per control: the seven fields. Cannot fill all seven? It is not a control yet.

DEPENDENCIES

Builds on M10 · hands to M12 + M13 · framework F06 Risk Anatomy

3 · GPAI PROVIDER REGISTER

One per estate: every model you ride, its Art 53/55 status, owner and re-check trigger.

STANDARDS ANCHORED

EU AI Act · NIST AI RMF · ISO/IEC 42001 · MS Responsible AI