

AI Guardrails and Agent Governance Assessment

A three week review of your Microsoft 365 and agent estate, with risks rated against evidence and a fix-it plan ordered by risk and effort.

3 Weeks

REVIEW TO PLAN

From \$22k

FIXED SCOPE

Board Ready

STATE OF PLAY REPORT

"Copilot went out to everyone. Now legal is asking questions I cannot answer."

WHY THIS HAPPENS

Copilot inherits every permission a user already has

Years of quiet oversharing sit dormant in SharePoint and Teams until something makes it easy to find. Then an agent gets built, a flow moves data somewhere it should not, and nobody has the full picture.

WHAT TO EXPECT

Three weeks, three stages

WEEK 1

Discovery

We review tenant configuration, your Copilot rollout, the agents and automations already running, and whatever governance documentation exists.

WEEK 2

Analysis

Sensitive data discovery through Microsoft Purview, an access and oversharing review across Entra ID and SharePoint, and a look at how agents are grounded and logged.

WEEK 3

Reporting and readout

We test the findings with your team, build the fix-it plan, then present it to your executive.

What you have at the end of week three

- ✓ **A written assessment** of your AI and agent estate, with risks rated and backed by evidence
- ✓ **A ranked fix-it plan** ordered by risk and by effort, so you can start on Monday
- ✓ **A draft governance framework** covering identity, data handling, logging, acceptable use and human oversight
- ✓ **A board-ready summary** of where you stand and what happens next



Written for two audiences at once

Detailed enough for a technology leader to act on, clear enough for a board to follow. That matters when AI risk is on the agenda but the detail sits several layers down.

PROOF**Governance we have put in place, not written about****MR****Medical Research
MS PURVIEW**

Nobody could say what research and personal data Copilot would surface.

We reviewed data protection against the risks that actually applied.

- ✓ Copilot went ahead with limits
- ✓ Data protection matched to risk

RC**Regional Council
POWER PLATFORM**

Power Platform had grown across seven environments with little governance.

We reviewed the setup and supported the changes that tightened it.

- ✓ Governance across 7 environments
- ✓ 1,400 monthly runs under control

CT**State Education
ID AND AUTOMATION**

Assigning Microsoft licences was a slow manual job that could not keep up with growing staff numbers.

We automated it from HR data.

- ✓ Licences assigned automatically
- ✓ Lower admin overhead and cost

WHY CG TECH**Who you are buying from****Brisbane based,
Australia wide**

An Australian team you can meet, delivering across Australia and the Pacific.

**Right tool for the job**

We work accross Microsoft, OpenAI, Anthropic, Perplexity and Open Source solutions.

**Approved government
supplier**

On Federal, State and Local Government ICT and Professionl Services panels.

BEFORE YOU COMMIT**The questions we get asked****Do we have to pause Copilot while you do this?**

No. The review runs alongside normal use. If we find something urgent in week one, you hear about it in week one rather than at the readout.

Will your team need broad access to our tenant?

Read access scoped to what the review needs, agreed in writing before we start. We do not need standing global admin.

What if you find something serious?

We tell you immediately and separately, not buried on page 40. The report is evidence-backed so you can act on it without re-litigating the finding.

SCAN TO BOOK**or call (07) 5641 1440**