CYBER SECURITY | AUSTRALIAN BUSINESS

# AI Governance and Shadow AI:
# A Practical Guide for Business Leaders

Understand the risk. Assess your controls. Take action.

kmtech.com.au | Cyber-First Managed Services | Melbourne

Artificial intelligence is reshaping how Australian businesses operate, but the same tools that boost productivity are creating invisible exposure to data breaches, regulatory penalties, and client trust erosion. This guide brings together the key risks, practical controls, and a 30-point governance checklist your leadership team can use today.

| 85% | 100% | 90%+ | 0 |
|---|---|---|---|
| Of daily business work happens in a browser | Of generative AI runs through the browser | Of browser-borne breaches stopped at source | Disruption to workflows with the right implementation |

THE RISK YOUR BUSINESS CANNOT SEE

## Shadow AI is happening right now, without a single alert firing.

**Privileged Data Leaving the Business**
Staff paste client briefs, financial records, and contracts into public AI tools like ChatGPT or Gemini. No firewall alert, no DLP trigger, no audit trail.

**AI-Crafted Phishing Attacks**
Generative AI produces spoofed login pages indistinguishable from Microsoft or your bank. One stolen password can cascade into a major incident.

**Compliance and Audit Exposure**
Regulators and insurers increasingly treat absence of evidence as potential exposure. No logs means no defence in a review, audit, or incident investigation.

**Ungoverned AI Sprawl**
Staff access ChatGPT, DeepSeek, Gemini, and others from firm devices simultaneously. No visibility, no governance, no control over what data leaves.

WHAT CONTROLLED AI ADOPTION GIVES YOUR BUSINESS

## From exposure to assurance, without disrupting how your team works.

**Shadow AI Governance**
Every AI tool accessed on every device is logged, categorised, and governed in real time. Unapproved AI sites blocked. Sensitive inputs flagged before they leave the device.

**Advanced Phishing Defence**
Visual AI analysis detects spoofed login pages using pixel patterns and page structure, not just URLs, stopping credential theft at the moment of click.

**Browser-Level Data Loss Prevention**
Control exactly what can leave the business via the browser. Block uploads to untrusted services and stop sensitive data being copied to unapproved platforms.

**Compliance-Grade Logging**
Every blocked event is timestamped and recorded (user, action, outcome) without storing actual content. When a regulator asks, you respond with evidence.

**Regulatory expectations are tightening.** Australian regulators, including ASIC, OAIC, and industry-specific bodies, expect businesses to demonstrate active, enforceable controls over AI usage and data handling. Documented evidence of appropriate controls protects your board, your professional indemnity insurer, and your clients.

AI GOVERNANCE CHECKLIST

# AI Governance Checklist

Score your organisation across 30 questions. Each Yes scores 1 point. Use this as a board-level readiness assessment or internal audit tool.

## SECTION 1 Governance and Policy

| YES | | QUESTION |
|---|---|---|
| ☐ | 1 | Does the organisation have a written policy covering staff use of AI tools (e.g. ChatGPT, Gemini, Copilot)? |
| ☐ | 1 | Is there a designated person or committee responsible for AI governance decisions and accountability? |
| ☐ | 1 | Does the policy differentiate between organisation-provided AI and public or personal AI tools? |
| ☐ | 1 | Has the AI policy been reviewed or updated in the past 12 months to reflect current tools and regulatory guidance? |
| ☐ | 1 | Is AI governance a standing agenda item at leadership or risk committee meetings? |

## SECTION 2 Data and Confidentiality

| YES | | QUESTION |
|---|---|---|
| ☐ | 1 | Have staff been formally instructed not to input client, customer, or sensitive data into public AI tools? |
| ☐ | 1 | Does the organisation know whether AI tools staff use store, retain, or share input data with third parties? |
| ☐ | 1 | Are there controls or written guidance covering what types of documents can and cannot be uploaded to AI platforms? |
| ☐ | 1 | Do systems provide any visibility over large copy-paste activity or bulk content transfers to web applications? |
| ☐ | 1 | Has the organisation considered how AI usage interacts with its obligations under the Privacy Act and confidentiality agreements? |

## SECTION 3 Visibility and Control

| YES | | QUESTION |
|---|---|---|
| ☐ | 1 | Does the organisation have any way to identify what AI tools (free or paid) being accessed on its devices or networks? |
| ☐ | 1 | Are there technical controls in place to block unapproved AI applications if required? |
| ☐ | 1 | Are existing cybersecurity measures (such as DLP or access controls) configured to address AI-related data flows? |
| ☐ | 1 | Does the organisation have browser-level visibility over which AI websites staff visit, and how frequently? |
| ☐ | 1 | Can the organisation produce a log or audit trail of AI tool usage if requested by a client, insurer, or regulator? |

## SECTION 4 Training and Staff Behaviour

| YES | | QUESTION |
|---|---|---|
| ☐ | 1 | Have all staff received training or communication covering acceptable AI use and associated risks? |
| ☐ | 1 | Do staff understand that AI outputs can contain errors, hallucinations, or fabricated information? |
| ☐ | 1 | Is there a clear, documented process for staff to request approval for a new AI tool before using it? |
| ☐ | 1 | Has the organisation addressed AI risks specifically in its professional development or induction programs? |
| ☐ | 1 | Do staff know who to contact if they suspect sensitive data has been submitted to an unapproved AI platform? |

## SECTION 5 Incident and Assurance Readiness

| YES | | QUESTION |
|---|---|---|

| | | |
|---|---|---|
| ☐ | 1 | Does the organisation have a documented response plan if a data incident occurs via an AI platform? |
| ☐ | 1 | Can the organisation demonstrate to a client, insurer, or regulator that it has active, enforceable AI controls? |
| ☐ | 1 | Is AI-related risk formally documented in the organisation's risk register or business continuity framework? |
| ☐ | 1 | Has the organisation reviewed its professional indemnity insurance coverage in the context of AI-related incidents? |
| ☐ | 1 | Are AI governance controls subject to periodic review or independent assurance? |

## SECTION 6 Regulatory and Compliance Alignment

| YES | | QUESTION |
|---|---|---|
| ☐ | 1 | Is the organisation aware of current Australian regulatory guidance (ASIC, OAIC, APRA) on AI and data governance? |
| ☐ | 1 | Has the organisation assessed its current AI practices against applicable regulatory expectations for technology risk? |
| ☐ | 1 | Are client confidentiality and Privacy Act obligations explicitly addressed in the AI acceptable use policy? |
| ☐ | 1 | Does the organisation's data environment have specific controls preventing exposure via AI-enabled browser activity? |
| ☐ | 1 | Has the organisation considered how emerging AI regulation (state, federal, or international) may affect its obligations? |

## SCORE YOUR RESULTS: HOW DOES YOUR ORGANISATION RATE?

| 0-8 | 9-16 | 17-24 | 25-30 |
|---|---|---|---|
| **High Risk** | **Partial Controls** | **Basic Foundation** | **Controlled** |
| Urgent action needed across policy, visibility, controls, and staff awareness. | Significant improvements needed before claiming controlled AI adoption. | Awareness exists but targeted uplift is needed in key areas. | Strong governance in place. Continue monitoring as tools and regulations evolve. |

### Book a Complimentary AI Governance Risk Review

Whatever your score, KMTech can help. Our AI Governance Risk Review maps your current gaps against applicable Australian regulatory expectations and gives you a prioritised action plan your leadership team can act on immediately.

**kmtech.com.au | info@kmtech.com.au**

**BOOK NOW**
**KMTECH.COM.AU**