CRO Brief

AI Governance & Risk Controls Checklist

Due Diligence Guide for:

Chief Risk Officers • Heads of Governance & Risk
Compliance Directors • Information Security Officers

BackPro AI
December 2025

www.backpro.ai

Purpose

This checklist provides Chief Risk Officers with a framework for evaluating AI vendors deploying in APRA-regulated superannuation funds. Use this to assess whether proposed AI implementations align with SPS 234 (data sovereignty), SPS 515 (operational risk), and governance requirements.

1 Data Sovereignty & SPS 234 Compliance

Critical Questions

Data Location & Processing

- Where is member data processed? (Must be: Australian infrastructure only)
- Does the solution make any external API calls? (Must be: No external calls)
- Can you provide network traffic logs showing zero offshore transmission?
- Is data encrypted at rest and in transit? What key management?

Deployment Architecture

- Is this deployed in our infrastructure or vendor's cloud?
- Do we maintain operational control over the deployment?
- Can we air-gap the deployment if required?
- Does the vendor access our member data? (Must be: No)

Red Flags

Reject if:

- Vendor requires member data transmission to their servers
- Solution relies on OpenAI, Anthropic, or Google cloud APIs
- Data processing location is "global" or "multi-region"
- Vendor cannot provide network isolation proof

2 Material Outsourcing (SPS 231)

Critical Questions

Service Provider Classification

- Is this a software licence or managed service?
- If vendor ceased operations, would our deployment continue functioning?
- Does the vendor perform operational activities on our behalf?
- Do we require APRA material service provider registration?

Operational Dependency

Can we operate if vendor support is unavailable?

Do we have source code escrow arrangements?

What is the exit/transition strategy?

Are we dependent on vendor's infrastructure?

Preferred Answer

Ideal scenario: Software licence model where we deploy in our infrastructure, vendor has no data access, and we maintain operational control. Avoids SPS 231 registration.

3 Operational Risk Framework (SPS 515)

Critical Questions

Risk Identification

What operational risks does AI introduce? (Accuracy, availability, dependency)

How do we monitor AI output quality?

What happens if AI generates incorrect information?

What is the fallback to manual processes?

Controls & Monitoring

Are human review workflows mandatory?

Can we enforce approval requirements before AI output goes live?

What accuracy metrics are tracked?

How are errors detected and corrected?

Risk Appetite Alignment

Does AI usage align with board-approved risk tolerance?

What is acceptable error rate for AI-generated content?

Which processes are suitable for automation vs. requiring human judgment?

How do we report AI risks to the board?

4 Audit Trail & Governance

Critical Questions

Transparency & Attribution

- Does every AI output include source attribution?
- Can we trace which documents informed each response?
- Are timestamps and user IDs logged for all AI interactions?
- Can we export audit logs for APRA examinations?

APRA Examination Readiness

- Can we demonstrate AI decision-making process to APRA?
- Do we have evidence of human oversight and approval?
- Can we show control effectiveness over 12-month period?
- Are audit trails tamper-proof and retained per policy?

5 Cyber Security (CPS 234)

Critical Questions

Access Controls

- Does AI integrate with our Azure AD / Entra ID?
- Is multi-factor authentication enforced?
- Can we implement role-based access controls?
- Are privileged access sessions logged and monitored?

Vulnerability Management

- How are security patches delivered and applied?
- Can we test patches in non-production before deployment?
- Is the vendor's security posture regularly assessed?
- Will AI be included in our penetration testing scope?

6 Implementation Governance

Pre-Deployment Approvals

Required Sign-Offs

Infrastructure: Architecture review and deployment approval

Security: CISO sign-off on access controls and encryption

Risk: Documented in operational risk register with controls

Compliance: APRA alignment confirmed (SPS 234, SPS 515, CPS 234)

Legal: Contract review (liability, IP, termination)

Board: Informed of AI deployment and residual risks

Post-Deployment Monitoring

Ongoing Oversight

Monthly: Review accuracy metrics, error rates, escalation volumes

Quarterly: Report to risk committee on AI operational risks

Annually: Internal audit of AI governance controls

Continuous: SIEM monitoring of AI access and usage patterns

Vendor Comparison Matrix

Use this to compare AI vendor proposals:

Criteria	Vendor A	Vendor B
Data processed in Australia	Yes / No	Yes / No
Zero external API calls	Yes / No	Yes / No
Software licence (not service)	Yes / No	Yes / No
Vendor has no data access	Yes / No	Yes / No
Complete audit trail	Yes / No	Yes / No
Human review workflows	Yes / No	Yes / No
Integrates with Azure AD	Yes / No	Yes / No
Can air-gap if required	Yes / No	Yes / No

Decision Framework

- All "Critical Questions" have satisfactory answers
- No red flags identified
- All required approvals obtained
- Residual risks align with board-approved risk appetite

- Any data sovereignty concerns
- Vendor requires member data transmission
- Cannot provide audit trail transparency
- Material outsourcing without APRA strategy

Contact BackPro

BackPro AI
Email: backpro@backpro.ai
Web: www.backpro.ai

Schedule a 30-minute governance walkthrough to address due diligence questions and demonstrate compliance controls.