CRO AI Governance Checklist

Due Diligence Framework for AI Vendor Evaluation

Essential Tool for:

Chief Risk Officers • Heads of Risk & Compliance
Executive General Managers Risk
Board Risk Committee Members

BackPro AI
December 2025

www.backpro.ai

Purpose

This checklist provides CROs with a structured framework for evaluating AI vendors proposed for claims automation or operational processes at APRA-regulated insurance companies.

Use this checklist to:

- Conduct vendor due diligence for Board Risk Committee approval
- Assess CPS 234 data sovereignty compliance
- Evaluate operational risk controls (CPS 230 alignment)
- Verify audit trail and explainability requirements
- Determine material outsourcing classification

1 Data Sovereignty & CPS 234 Compliance

1.1 Data Residency

Critical Questions:
☐ **Where is customer data processed?**
Must be: Within Australian jurisdiction (on-premise or Australian cloud regions)
Red flag: Offshore processing, multi-region data flows, unclear data residency
☐ **Are there any external API calls with customer data?**
Must be: Zero external API calls containing customer information
Red flag: Calls to US/European AI services, third-party analytics platforms
☐ **How is data stored at rest?**
Must be: Encrypted (AES-256 minimum) within your controlled infrastructure
Red flag: Vendor-controlled storage, unclear encryption standards
☐ **Can the vendor access customer data?**
Must be: No vendor access to customer data in production environment
Red flag: Vendor support requires access to live customer data

1.2 Deployment Architecture

☐ **Is deployment on-premise or within your cloud tenant?**
Acceptable: Deployed within your Azure/AWS/GCP subscription or on-premise
Red flag: SaaS model requiring data upload to vendor infrastructure
☐ **Who controls the infrastructure?**
Must be: Your IT operations team controls deployment, patching, access
Red flag: Vendor-managed infrastructure with your data
☐ **What happens to data if contract terminates?**
Must be: All data remains in your custody; software continues operating
Red flag: Data deletion obligations, vendor retains copies

2 Material Outsourcing Classification

2.1 Service vs Software Classification

☐ **Does vendor provide service or software?**
Software (no APRA notification): Tool deployed on your infrastructure for your staff
Service (APRA notification required): Vendor operates process on their infrastructure
☐ **Who maintains operational control of claims decisions?**
Must be: Your claims assessors make final decisions using AI as a tool
Red flag: Vendor makes automated decisions without your oversight
☐ **Is this a material business activity?**
Assessment: Claims processing is material—requires software licence model
Red flag: Vendor describes as "claims processing service" rather than software

3 Audit Trails & Explainability

3.1 Decision Transparency

☐ **Can AI explain every decision?**
Must be: Full source attribution (policy clauses, document references)
Red flag: Black-box AI, confidence scores without reasoning
☐ **What audit trail is captured?**
Minimum: Timestamp, user, input documents, decision logic, output, review notes
Red flag: Insufficient logging for APRA prudential review
☐ **Can audit trails be exported for APRA examination?**
Must be: Export to PDF, CSV, JSON for regulatory submission
Red flag: No export capability, vendor-only access to logs
☐ **How long are audit trails retained?**
Minimum: 7 years aligned with APRA record-keeping requirements
Red flag: Short retention periods, automatic log deletion

4 Operational Risk & CPS 230 Alignment

4.1 Control Framework

☐ **Does solution fit within your operational risk framework?**
Must be: Documented risk identification, controls, monitoring procedures
Red flag: New risk categories requiring framework restructure
☐ **What quality monitoring is available?**
Minimum: Real-time dashboards tracking assessment accuracy, escalation rates
Red flag: No quality metrics, manual monitoring required
☐ **How are errors and exceptions handled?**
Must be: Defined escalation procedures, human review for ambiguous cases
Red flag: Automatic decisions without human review option
☐ **What happens during system downtime?**
Must be: Documented fallback procedures, claims processing continuity
Red flag: No business continuity plan, single point of failure

4.2 Change Management

☐ **How are AI model updates deployed?**
Must be: Your change management process, testing environment, rollback capability
Red flag: Vendor pushes updates automatically, no testing phase
☐ **Can updates be deferred for testing?**
Must be: You control deployment timing and validation
Red flag: Mandatory immediate updates, no version control

5 Board Governance & Reporting

5.1 Board Risk Committee Requirements

☐ **Is a governance framework provided?**
Must be: Pre-built templates for Board reporting, risk appetite statements
Red flag: You must build governance framework from scratch
☐ **What Board reporting is available?**
Minimum: Quarterly Board Risk Committee pack with control effectiveness metrics
Red flag: No standard reporting, requires manual compilation
☐ **How is AI risk articulated to the Board?**
Must be: Clear risk categories, mitigation controls, residual risk assessment
Red flag: Technical jargon, unclear risk exposure

6 Implementation Risk

6.1 Deployment Complexity

☐ **What is the deployment timeline?**
Acceptable: 4-8 weeks including integration, testing, training
Red flag: Multi-month implementations, complex system dependencies
☐ **What integration is required?**
Minimum: API integration with claims systems (Guidewire, Duck Creek)
Red flag: Requires replacing core systems, major IT projects
☐ **What staff training is needed?**
Must be: Comprehensive training for claims assessors and IT operations
Red flag: Minimal training, "self-service" implementation
☐ **Is a pilot program possible?**
Must be: Pilot with one claim type (motor vehicle) before full rollout
Red flag: All-or-nothing deployment, no pilot option

7 Commercial & Legal

7.1 Contractual Protections

☐ **Are APRA prudential standards referenced in contract?**
Must be: Explicit CPS 234, 230, 220 compliance obligations
Red flag: Generic terms without regulatory requirements
☐ **What are termination and exit provisions?**
Must be: You retain all data, software continues operating, knowledge transfer
Red flag: Data deletion requirements, vendor lock-in
☐ **Who owns the audit trails and outputs?**
Must be: You own all AI outputs, audit trails, and derivative data
Red flag: Vendor retains rights to data or outputs
☐ **What liability is accepted for errors?**
Minimum: Professional indemnity insurance, defined liability caps
Red flag: Disclaimer of all liability, no insurance coverage

8 Vendor Stability & Support

☐ **Does vendor understand APRA requirements?**
Must be: Deep knowledge of CPS 234, 230, 220; Australian insurance experience
Red flag: Generic AI vendor with no regulatory expertise
☐ **What ongoing support is provided?**
Minimum: 24/7 technical support, dedicated account management, regulatory updates
Red flag: Email-only support, no SLA commitments
☐ **How are regulatory changes handled?**
Must be: Vendor monitors APRA updates, proactive compliance notifications
Red flag: You must identify compliance changes independently

Scoring & Decision Framework

Critical Requirements (Must Pass All)

Any "red flags" in these areas require vendor to remediate before proceeding:

- Data sovereignty (Section 1)
- Material outsourcing classification (Section 2)
- Audit trail capabilities (Section 3)

Recommended Approval Criteria

Proceed to Board Risk Committee:

- All critical requirements met
- Minimum 80% of operational risk checks passed (Section 4)
- Board governance framework provided (Section 5)
- Acceptable implementation risk (Section 6)

Require Vendor Remediation:

- Critical requirements have red flags
- Less than 60% operational risk checks passed
- High implementation risk without mitigation plan

Do Not Proceed:

- Data sovereignty cannot be assured
- Classified as material outsourcing without APRA notification plan
- No audit trail or explainability capability

Using This Checklist

1. **Vendor Evaluation:** Use during RFP process to assess AI vendor proposals
2. **Due Diligence:** Complete checklist before Board Risk Committee presentation
3. **Contract Negotiation:** Reference checklist requirements in vendor agreements
4. **Ongoing Oversight:** Re-evaluate annually or when vendor makes material changes

BackPro AI Assessment
BackPro AI is designed to pass all sections of this checklist:

✓ On-premise deployment within your Australian infrastructure (Section 1)

✓ Software licence model avoiding material outsourcing (Section 2)

✓ Complete audit trails with full explainability (Section 3)

✓ Pre-built governance framework and Board reporting (Sections 4-5)

Contact us for detailed due diligence documentation: www.backpro.ai