# AI & APRA Compliance for Insurers

Comprehensive Guide to Claims Automation Under CPS 234

**Essential Reading for:**

Chief Risk Officers • Heads of Claims Operations
Chief Information Security Officers • Board Risk Committee Members
Executive General Managers Risk & Compliance

BackPro AI
December 2025

www.backpro.ai

# Contents

# 1 Executive Summary

Australian insurance companies face mounting pressure to automate claims processing: customer expectations for rapid settlement, operational cost pressures from CFOs, and competitive threats from insurtech challengers using AI.

Yet CROs appropriately block most AI initiatives due to APRA CPS 234 data sovereignty violations. Cloud AI services (ChatGPT, Claude, Gemini) send customer medical records, financial information, and claims documents offshore—creating immediate compliance breaches.

This whitepaper provides a roadmap for deploying AI claims automation while maintaining complete APRA prudential compliance.

## 1.1 Key Findings

- **On-premise deployment** enables claims automation without CPS 234 violations
- **Software licence model** avoids material outsourcing registration requirements
- **Explainable AI** with complete audit trails supports APRA prudential reviews
- **CPS 230 integration** fits AI within existing operational risk frameworks
- **Board governance templates** enable rapid Risk Committee approval

## 1.2 Document Structure

1. APRA prudential standards overview (CPS 220, 230, 234)
2. Data sovereignty requirements for claims automation
3. Operational due diligence framework
4. Material outsourcing classification guidance
5. AI governance and Board Risk Committee oversight
6. Implementation roadmap and change management
7. Future regulatory considerations

# 2 APRA Prudential Standards for Insurance

## 2.1 CPS 220: Risk Management

CPS 220 (Risk Management) requires general and life insurers to:

**Risk Management Strategy:**

- Identify material risks to insurer operations
- Define risk appetite and tolerance levels
- Establish risk management framework with Board approval
- Monitor risk profile against appetite statements

**AI Claims Automation Risk Classification:**
AI-powered claims assessment creates operational risk requiring governance:

**CPS 220 Risk Assessment**

**Risk Category:** Operational Risk—Technology & Process Change

**Material Risk:** Yes—claims processing is core insurance activity

**Risk Appetite:** "Leverageadvanced technology to improve claims efficiency while maintaining complete human oversight of complex claims requiring judgment"

**Key Risks:**

- Model accuracy risk (incorrect claims assessments)
- Customer detriment risk (automated decisions without proper oversight)
- Regulatory risk (non-compliance with claims handling obligations)
- Operational resilience risk (system downtime affecting claims processing)

**Mitigating Controls:**

- Human review of all complex claims
- Defined escalation thresholds based on claim value and ambiguity
- Quality monitoring dashboards tracking assessment accuracy
- Documented fallback procedures for system downtime

## 2.2 CPS 230: Operational Risk Management

CPS 230 (Operational Risk Management, effective July 2023) introduces enhanced requirements:
**Control Environment:**

- Three lines of defence model for operational risk
- Service provider management and oversight
- Business continuity and operational resilience
- Regular testing of operational controls

**AI Claims Automation Control Framework:**

CPS 230 Three Lines of Defence

**First Line: Claims Operations**

- Claims assessors review AI recommendations with human oversight
- Quality assurance team validates AI assessment accuracy
- Escalation procedures for ambiguous or complex claims
- Daily monitoring of AI system availability and performance

**Second Line: Risk & Compliance**

- CRO oversight of AI governance framework
- Compliance monitoring of claims handling obligations
- Operational risk reporting to Executive Risk Committee
- Testing of AI control effectiveness

**Third Line: Internal Audit**

- Independent audit of AI claims assessment controls
- Testing of escalation procedures and human oversight
- Validation of audit trail completeness
- Board Audit Committee reporting on control effectiveness

### 2.3 CPS 234: Information Security

CPS 234 (Management of Information Security) is the primary compliance barrier for cloud AI adoption.

**Core Requirements:**

1. **Information Asset Classification:** Identify and classify information assets based on criticality and sensitivity
2. **Information Security Controls:** Implement controls appropriate to asset classification
3. **Third-Party Access:** Manage risks from third-party access to information assets
4. **Incident Response:** Detect, manage, and report information security incidents
5. **Operational Resilience:** Maintain security during business disruption

**Claims Data Classification Under CPS 234:**

## 3 Data Sovereignty Requirements

### 3.1 The Cloud AI Compliance Problem

Standard cloud AI services violate CPS 234 when processing claims:

| Data Type | Classification | Required Controls |
|---|---|---|
| Medical reports | Highly Confidential | Encryption (AES-256), access logging, Australian data residency, need-to-know access |
| Claim forms | Confidential | Encryption, audit logging, controlled access |
| Policy documents | Confidential | Encryption, version control, access controls |
| Photos/evidence | Confidential | Encrypted storage, access logging |
| Assessment notes | Internal | Access controls, audit trails |

**CPS 234 Violations: Cloud AI Services**

**OpenAI ChatGPT:**

- API calls send claims documents to US servers
- Customer medical and financial data processed offshore
- No data residency guarantees
- OpenAI retains rights to use data for model training (unless Enterprise plan)

**Anthropic Claude:**

- API hosted in US and Europe (no Australian region)
- Claims text sent to Anthropic infrastructure
- Data retention policies unclear for Australian customers

**Google Gemini:**

- Multi-region processing with data residency uncertainty
- Google Cloud terms permit cross-border data transfer
- Policy documents containing customer identifiers processed globally

**Result:** APRA requires notification of offshore data processing. CROs must report CPS 234 information security incidents for unauthorized offshore data transfer.

### 3.2 On-Premise AI Architecture

Alternative architecture maintaining complete data sovereignty:

**Compliant Architecture: On-Premise Deployment**

**Deployment Model:**

1. AI software deployed within your controlled infrastructure
2. Choose: Azure Australia, AWS Sydney, GCP Sydney, or on-premise data center
3. All AI models, processing, and data remain in your environment
4. Zero external API calls containing customer data

**Data Flow:**

1. Claims assessor opens claim in Guidewire/Duck Creek
2. Claims system calls AI API within your infrastructure
3. AI accesses claims documents from your document management system
4. Processing occurs entirely within your controlled environment
5. Results returned to claims system—customer data never leaves your infrastructure

**CPS 234 Compliance:**

Customer data remains in Australian jurisdiction

No offshore data processing or storage

Your existing access controls and audit logging maintained

No third-party access to customer information

Information security controls remain under your control

# 4 Material Outsourcing Classification

## 4.1 APRA Outsourcing Requirements

APRA distinguishes between material and non-material outsourcing:

**Material Outsourcing (CPS 231):**

> *"An arrangement under which an insurer relies on a service provider (related or unrelated) to undertake a business activity that forms part of the insurer's operations and is critical to the insurer's ability to manage prudential risks or maintain operational performance."*

**APRA Notification Requirements:**

- Notification to APRA before material outsourcing commences
- Due diligence on service provider financial strength and capability
- Contractual protections including audit rights and termination clauses
- Ongoing monitoring of service provider performance
- Board approval of material outsourcing arrangements

### 4.2 Software Licence vs Service Provider

AI claims automation classification depends on operational control:

| **Material Outsourcing (APRA notification required)** | **Software Licence (No APRA notification)** |
|---|---|
| Third-party operates claims processing service | Software tool deployed on your infrastructure |
| Vendor makes claims decisions | Your staff make decisions using software |
| Customer data processed on vendor infrastructure | Customer data stays in your environment |
| Vendor controls process and systems | You control deployment and operations |
| Service contract (ongoing services) | Software licence (you operate software) |

### 4.3 BackPro AI Classification

**Why BackPro AI is NOT Material Outsourcing:**

1. **Operational Control:** Your claims assessors retain decision-making authority. AI provides recommendations; humans make final claims decisions.
2. **Infrastructure Control:** Deployed on your infrastructure (Azure/AWS/GCP tenant or on-premise). Your IT team controls deployment, patching, access.
3. **Data Custody:** All customer data remains in your custody. BackPro software processes data within your environment—vendor has no access.
4. **Software Tool:** BackPro provides software functionality, not claims processing services. Comparable to claims management system or policy administration software.

**CRO Due Diligence Approach:**
Even without material outsourcing classification, conduct operational due diligence:

- Vendor financial stability and support capability
- Software security testing (penetration testing, code review)
- Integration architecture review
- Business continuity and disaster recovery procedures
- Contract terms including liability, termination, IP ownership

## 5 Explainability & Audit Trails

### 5.1 APRA Prudential Review Requirements

When APRA conducts prudential reviews, insurers must demonstrate:
**Claims Decision Transparency:**

- How claims decisions were reached
- Policy clauses applied to specific claims

- Assessment reasoning and evidence considered
- Human oversight of automated recommendations

**Control Effectiveness:**

- Evidence that escalation procedures operate effectively
- Testing results of AI accuracy against human assessors
- Quality monitoring processes and results
- Training provided to claims assessors

### 5.2 Explainable AI Architecture

Requirements for APRA-compliant AI:

**Explainable AI Requirements**

**Every AI Assessment Must Include:**

1. **Source Attribution:** Exact policy clauses applied with policy section references
2. **Document References:** Which claims documents were analysed (claim form, photos, medical reports, quotes)
3. **Decision Logic:** Step-by-step reasoning from evidence to conclusion
4. **Confidence Score:** Quantified confidence in recommendation (triggers escalation if low)
5. **Escalation Triggers:** Why claim was flagged for human review (ambiguity, high value, policy interpretation uncertainty)
6. **Human Review Notes:** Claims assessor comments if overriding AI recommendation

**Audit Trail Retention:**

- Minimum 7-year retention aligned with APRA record-keeping requirements
- Export capabilities: PDF (individual claims), CSV (bulk analysis), JSON (system integration)
- Searchable by claim ID, assessor, date range, claim type
- Immutable logging preventing retroactive modification

## 6 Board Risk Committee Governance

### 6.1 AI Governance Framework

Board Risk Committee approval requires documented governance:

**Governance Structure:**

1. **Board Risk Committee:**
   - Approves AI adoption for claims processing

- Sets risk appetite for AI assessment accuracy
- Reviews quarterly reports on AI control effectiveness
- Oversees material changes to AI scope or capability

2. **Executive Risk Committee:**

- Monthly review of AI quality metrics
- Oversight of escalation rate trends
- Approval of AI model updates
- Monitoring of operational risk indicators

3. **AI Steering Committee:**

- Claims Operations, Risk, Compliance, IT representatives
- Operational oversight of AI deployment
- Review of assessor feedback and system improvements
- Coordination of testing and quality assurance

4. **Claims Operations:**

- Day-to-day monitoring of AI performance
- Quality assurance testing and validation
- Assessor training and change management
- Incident response and issue escalation

### 6.2 Risk Appetite Statement

Example Board-approved risk appetite for AI claims automation:

**AI Risk Appetite Statement**

AI may be used for automated assessment of straightforward claims (motor vehicle, home & contents, standard life insurance) where:

- AI assessment accuracy exceeds 95% for claim type (validated quarterly)
- Complete audit trails enable full explainability of decisions
- Claims above $25,000 or involving medical interpretation require mandatory human review
- Ambiguous policy clauses or novel claim scenarios escalate to experienced assessors
- Customer disputes result in immediate human re-assessment

The CRO is responsible for AI governance framework, control effectiveness monitoring, and quarterly Board Risk Committee reporting on AI operational risk." *"The insurer will leverage artificial intelligence to improve claims processing efficiency, consistency, and customer experience while maintaining complete human oversight of complex claims requiring professional judgment.*
*AI may be used for automated assessment of straightforward claims (motor vehicle, home & contents, standard life insurance) where:*

- *AI assessment accuracy exceeds 95% for claim type (validated quarterly)*
- *Complete audit trails enable full explainability of decisions*
- *Claims above $25,000 or involving medical interpretation require mandatory human review*
- *Ambiguous policy clauses or novel claim scenarios escalate to experienced assessors*
- *Customer disputes result in immediate human re-assessment*

*The CRO is responsible for AI governance framework, control effectiveness monitoring, and quarterly Board Risk Committee reporting on AI operational risk."*

# 7 Implementation Roadmap

## 7.1 Phase 1: Due Diligence & Planning (Weeks 1-2)

**CRO Activities:**

- Complete vendor due diligence checklist (data sovereignty, audit trails, controls)
- CPS 234 compliance assessment—validate on-premise deployment architecture
- Material outsourcing classification determination
- Draft AI governance framework for Board Risk Committee review
- Prepare Board Risk Committee paper with risk assessment and mitigation plan

**Claims Operations Activities:**

- Select pilot claim type (typically motor vehicle claims)

- Define success criteria (processing time, accuracy, customer satisfaction)
- Identify pilot team (5-10 claims assessors)
- Document current state metrics (claims per day, average processing time, cost per claim)

### 7.2 Phase 2: Technical Deployment (Weeks 3-4)

**IT Implementation:**

- Deploy AI software within Australian infrastructure (Azure/AWS/GCP)
- Configure API integration with claims management system
- Connect to document management system for claims document access
- Implement access controls and audit logging
- Penetration testing and security validation

**Testing & Validation:**

- Parallel run: AI assesses historical claims, compare to actual assessor decisions
- Accuracy validation across 200+ claims
- Edge case testing (ambiguous policy clauses, unusual claims scenarios)
- Performance testing (claims processing throughput, system response time)

### 7.3 Phase 3: Pilot & Governance (Weeks 5-6)

**Pilot Program:**

- Pilot team uses AI for motor vehicle claims assessment
- Daily monitoring of accuracy, escalation rates, processing time
- Weekly retrospective reviews with claims assessors
- Collect assessor feedback on AI recommendations and user experience

**Board Approval:**

- Board Risk Committee presentation with pilot results
- Risk appetite statement approval
- AI governance framework ratification
- Approval to proceed to production rollout

### 7.4 Phase 4: Production Rollout (Weeks 7-10)

**Expansion Strategy:**

1. **Week 7:** All motor vehicle claims (pilot team + 10 additional assessors)
2. **Week 8:** Add home & contents claims
3. **Week 9:** Add income protection claims
4. **Week 10:** Add straightforward life insurance claims

**Change Management:**

- Comprehensive training for all claims assessors
- Documentation of escalation procedures and human override processes
- Communication to customers about enhanced claims processing
- Ongoing monitoring and continuous improvement

## 8 Future Regulatory Considerations

### 8.1 APRA AI Guidance Development

APRA has not issued AI-specific prudential standards, but future guidance expected:

**Likely Areas of Focus:**

- Model risk management for AI/ML systems
- Algorithmic bias testing and fairness requirements
- Consumer protection for automated decision-making
- Enhanced explainability standards
- Third-party AI model validation requirements

**Preparing for Future Requirements:**

- Establish robust AI governance framework now
- Document model development, testing, and validation procedures
- Maintain comprehensive audit trails and decision logs
- Test for bias in claims assessment across customer demographics
- Ensure complete explainability of all AI recommendations

### 8.2 International Regulatory Trends

Australian insurers should monitor international AI regulation:

**EU AI Act:**

- High-risk AI systems require conformity assessment
- Claims decision-making likely classified as high-risk
- Transparency and explainability mandated
- Human oversight requirements

**UK AI Regulation:**

- FCA and PRA principles-based approach
- Focus on consumer protection and fairness
- Model risk management frameworks

## 9 Conclusion

AI-powered claims automation is achievable while maintaining complete APRA compliance through:

1. **On-premise deployment** maintaining CPS 234 data sovereignty
2. **Software licence model** avoiding material outsourcing registration
3. **Explainable AI** with comprehensive audit trails for APRA reviews
4. **CPS 230 integration** fitting AI within operational risk framework
5. **Board governance** providing Risk Committee oversight and control

**CRO Action Items:**

1. Evaluate AI vendors using due diligence checklist (Appendix A)
2. Validate CPS 234 compliance through on-premise deployment verification
3. Develop Board Risk Committee paper with risk appetite and governance framework
4. Coordinate pilot program with Claims Operations
5. Monitor regulatory developments and adjust governance as needed

**About BackPro AI**

BackPro AI provides on-premise claims automation software purpose-built for APRA-regulated insurance companies. Our solution enables:

- 60% reduction in claims processing time
- Complete CPS 234 data sovereignty compliance
- Full audit trails for APRA prudential reviews
- Pre-built governance framework for Board approval

Contact us for technical due diligence documentation and pilot program planning: **www.backpro.ai**