APRA SPS 234 Compliance Framework

Technical Brief: Data Sovereignty & On-Premise AI

Essential Reading for:

Chief Risk Officers • Executive General Manager Risk & Compliance
Head of Governance & Risk • APRA Reporting Managers

BackPro AI
December 2025

www.backpro.ai

Contents

1 Executive Summary **2**

2 APRA SPS 234 Requirements Overview **2**
2.1 Information Security Controls 2
2.2 The Cloud AI Problem 2

3 On-Premise AI Architecture **3**
3.1 Complete Data Sovereignty 3
3.2 Information Security Controls 3

4 Material Outsourcing Classification **3**
4.1 SPS 231 Material Service Provider Rules 3
4.2 Why BackPro Is Not Material Outsourcing 3

5 Operational Risk Framework (SPS 515) **4**
5.1 Integration With Risk Management 4
5.2 Operational Resilience (SPS 232) 4

6 Cyber Security Alignment (CPS 234) **4**
6.1 Information Asset Classification 4
6.2 Security Controls Implementation 5

7 Audit Trail & APRA Examination Readiness **5**
7.1 Complete Source Attribution 5
7.2 APRA Prudential Review Evidence 5

8 Implementation Governance **5**
8.1 Pre-Deployment Checklist 5
8.2 Ongoing Monitoring 6

9 Conclusion **6**
9.1 Next Steps 6

1 Executive Summary

Australian superannuation funds face a critical technology dilemma: AI-powered automation offers substantial operational efficiencies, but cloud-based AI services (ChatGPT, Claude, Gemini) create immediate APRA SPS 234 compliance violations by sending member data offshore.

BackPro AI solves this through complete on-premise deployment within your controlled Australian infrastructure. All member data, compliance records, and regulatory submissions stay in your environment with zero external API calls.

This framework covers:

- APRA SPS 234 data sovereignty requirements
- How on-premise AI maintains information security controls
- Material outsourcing classification and why BackPro avoids it
- Operational resilience under SPS 232
- Audit trail requirements for APRA prudential reviews

2 APRA SPS 234 Requirements Overview

2.1 Information Security Controls

APRA Prudential Standard SPS 234 (Management of Security Risk) requires RSE licensees to:

1. **Maintain information security:** Implement controls to protect information assets, including member data, from unauthorized access, misuse, interference, loss, and unauthorized modification or disclosure.
2. **Control third-party access:** Where service providers require access to information assets, the RSE licensee must maintain adequate contractual protections and oversight mechanisms.
3. **Data sovereignty:** Member data and fund operational information must be stored and processed within Australia, or with explicit APRA notification if overseas processing occurs.
4. **Incident response:** Documented procedures for identifying, managing, and reporting information security incidents to APRA within required timeframes.

2.2 The Cloud AI Problem

Standard cloud AI services create SPS 234 violations:

- **ChatGPT (OpenAI):** Sends queries to US servers. Member data leaves Australian jurisdiction. Privacy policy states data may be used for model training.
- **Claude (Anthropic):** US-based processing. No Australian data residency option. Constitutional AI training may involve query data.
- **Gemini (Google):** Global data centres with unclear routing. Member data processed offshore without RSE licensee control.

Compliance Gap: These services constitute material outsourcing arrangements requiring APRA notification, yet provide insufficient contractual protections for member data sovereignty.

3 On-Premise AI Architecture

3.1 Complete Data Sovereignty

BackPro AI deploys entirely within your infrastructure:

1. **Installation:** Deploy on Azure Australia East, AWS Sydney, or GCP Sydney regions within your tenant.
2. **Data access:** AI accesses member records, administration systems, and financial data through your existing APIs and database connections.
3. **Processing:** All natural language processing, document generation, and query responses occur within your controlled environment.
4. **Zero external calls:** No API calls to external AI services. No member data transmission outside your infrastructure.

3.2 Information Security Controls

Your existing controls apply to BackPro:

- **Access controls:** BackPro inherits your Azure AD / Entra ID authentication and authorization rules.
- **Audit logging:** All AI queries and responses logged through your existing SIEM (Splunk, Azure Sentinel, etc.).
- **Network isolation:** Deploy in private VNet/VPC with no internet egress. Air-gapped if required.
- **Encryption:** Data encrypted at rest using your key management (Azure Key Vault, AWS KMS). TLS 1.3 in transit.

4 Material Outsourcing Classification

4.1 SPS 231 Material Service Provider Rules

APRA SPS 231 defines a material service provider as an entity performing activities that, if disrupted, would significantly impact the RSE licensee's operations.

Cloud AI services would typically qualify as material:

- Service disruption stops AI-dependent processes
- Provider has access to member data
- Operational dependence creates concentration risk

4.2 Why BackPro Is Not Material Outsourcing

BackPro operates as a **software licence**, not a service provider:

1. **No data access:** BackPro (the vendor) never accesses your member data. Software runs in your environment with your credentials.
2. **No operational control:** You maintain full control over deployment, configuration, and operations. BackPro provides software updates, not operational services.

3. **No dependency:** If BackPro (vendor) ceased operations, your deployed instance continues functioning. You own the deployment.

4. **Your infrastructure:** Software runs on your servers, using your compute resources, within your security boundary.

Classification: Software licence purchase, similar to Microsoft Office or Adobe Acrobat. Does not require SPS 231 material service provider registration.

5 Operational Risk Framework (SPS 515)

5.1 Integration With Risk Management

APRA SPS 515 requires RSE licensees to maintain an operational risk management framework. BackPro fits within this framework:

- **Risk identification:** Document AI usage in operational risk register (e.g., accuracy risk, availability risk, staff dependency).
- **Controls:** Human review workflows, output validation checks, fallback procedures to manual processes.
- **Monitoring:** Track AI response accuracy rates, escalation volumes, and error correction cycles.
- **Risk tolerance:** Align AI deployment with board-approved operational risk appetite statement.

5.2 Operational Resilience (SPS 232)

BackPro deployment aligns with business continuity requirements:

1. **Disaster recovery:** Deploy in your existing DR environment. Failover to secondary region follows your DR plan.
2. **Backup and restore:** BackPro configuration backed up alongside other application infrastructure.
3. **RTO/RPO alignment:** Software availability tied to your infrastructure RTO. No external dependency for recovery.
4. **Testing:** Include BackPro in annual DR testing scenarios.

6 Cyber Security Alignment (CPS 234)

6.1 Information Asset Classification

Under APRA CPS 234 (Information Security), BackPro processes:

- **Member data:** Account balances, contribution records, insurance details (High sensitivity)
- **Fund policies:** PDSs, insurance policies, investment guides (Medium sensitivity)
- **Operational data:** Query logs, response accuracy metrics (Low sensitivity)

6.2 Security Controls Implementation

BackPro inherits your CPS 234 controls:

1. **Access management:** Multi-factor authentication via your identity provider. Role-based access controls.
2. **Vulnerability management:** BackPro security updates deployed through your change management process.
3. **Penetration testing:** Include BackPro in annual penetration testing scope.
4. **Incident response:** BackPro security incidents escalated through your existing CSIRT procedures.

7 Audit Trail & APRA Examination Readiness

7.1 Complete Source Attribution

Every AI-generated response includes:

- **Source documents:** References to specific PDSs, policy documents, member records used
- **Timestamps:** When query received, when response generated, when human reviewed
- **User attribution:** Which staff member initiated query, who approved output
- **Version control:** Document versions used in response generation

7.2 APRA Prudential Review Evidence

Export compliance reports formatted for APRA examiners:

1. **AI decision-making transparency:** Show which data informed each response
2. **Human oversight:** Demonstrate review and approval workflows
3. **Accuracy tracking:** Report error rates, correction cycles, quality metrics
4. **Control effectiveness:** Evidence that governance controls operate as designed

8 Implementation Governance

8.1 Pre-Deployment Checklist

Before deploying BackPro, confirm:

Infrastructure team approved deployment architecture

Security team validated access controls and encryption

Risk team documented operational risks and controls

Compliance team reviewed APRA SPS 234 alignment

$$ Legal reviewed software licence terms

Board informed of AI deployment and risk mitigation

8.2 Ongoing Monitoring

Establish monitoring cadence:

- **Monthly:** Review AI accuracy metrics, escalation volumes, error corrections
- **Quarterly:** Report to risk committee on operational risk indicators
- **Annually:** Internal audit review of AI governance controls
- **As-needed:** APRA notification if material changes to AI usage

9 Conclusion

APRA SPS 234 compliance does not preclude AI adoption in superannuation funds. On-premise deployment maintains complete data sovereignty while delivering operational efficiency benefits.

BackPro AI enables automation of APRA reporting, regulatory monitoring, and trustee documentation without compromising member data security or creating material outsourcing arrangements.

9.1 Next Steps

1. **Technical architecture review:** Validate deployment approach with your infrastructure team (30 minutes)
2. **Security assessment:** Walk through access controls, encryption, and audit trails with CISO (45 minutes)
3. **Pilot deployment:** 2-4 week pilot in non-production environment to validate controls
4. **Governance approval:** Present to risk committee for deployment authorization

Contact

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

Schedule a 30-minute compliance walkthrough to demonstrate SPS 234 controls and audit trail capabilities.