Governance, Risk & Compliance Requirements - Invoice Processing Automation

Regulatory Compliance

Our organization must comply with: - **Australian Taxation Office (ATO)** requirements for invoice retention and GST reporting - **Corporations Act 2001** for financial record keeping (7-year retention) - **Privacy Act 1988** for handling vendor personal information - **Payment Card Industry Data Security Standard (PCI-DSS)** for payment processing

We operate only within Australia, so GDPR does not apply. However, some of our vendors are international, requiring careful handling of cross-border data considerations.

Data Governance

Data Ownership: - Finance team owns invoice data - Procurement owns vendor master data - IT manages data infrastructure

Data Classification: - **Confidential**: Vendor bank account details, pricing agreements - **Internal**: Invoice amounts, PO numbers, approval workflows - **Public**: Vendor company names, addresses

We have a **data quality team** that performs quarterly audits, but data lineage tracking is manual and inconsistent. Master data management is handled through SAP, but synchronization with other systems is a known issue.

Risk Management

Our enterprise risk management framework is based on ISO 31000. Risk appetite for automation: - **High tolerance**: Process automation for standard invoices - **Medium tolerance**: AI-driven decision making with human oversight - **Low tolerance**: Fully autonomous payment approvals without review

Key Risks Identified: - Data breach exposing vendor financial information (High impact, Medium likelihood) - AI model making incorrect payment decisions (Medium impact, Medium likelihood) - System downtime during month-end processing (High impact, Low likelihood) - Vendor fraud through invoice manipulation (High impact, Low likelihood)

We have cyber insurance coverage up to $5M, but AI-specific liability coverage is not yet in place.

Audit & Traceability

Audit Requirements: - Internal audit: Quarterly reviews of payment processes - External audit: Annual financial statement audit by PwC - ATO audit: Ad-hoc, typically every 3-4 years

Traceability Needs: - Complete audit trail of invoice status changes - User actions and approvals with timestamps - AI decision explanations for exception handling - Immutable logs for compliance purposes

Current audit trail is stored in Oracle database with 7-year retention. We need to demonstrate "right to explanation" for any automated decisions that affect vendor payments.

Security Governance

Security Certifications: - ISO 27001 certified (renewed annually) - SOC 2 Type II report (last completed 18 months ago)

Security Assessments: - Annual penetration testing by external firm - Quarterly vulnerability scans - Monthly security awareness training for all staff

Incident Response: We have a documented incident response plan with 4-hour notification requirement for data breaches. Security Operations Center (SOC) operates during business hours only.

Change Management & Approval

Change Approval Board (CAB): - Meets weekly to review production changes - Requires 5 business days notice for standard changes - Emergency changes require CIO approval

Deployment Approval: - UAT sign-off required from business owner - Security review for any new integrations - Compliance review for changes affecting financial reporting

Impact Assessment: We use a standard template to assess business, technical, and security impacts. High-impact changes require executive approval.

Note: This document covers regulatory compliance and risk management basics. Missing information includes detailed AI governance framework, model explainability requirements, bias detection processes, model versioning procedures, and comprehensive third-party risk management approach.