ACME INC

BACKUP POLICY APPENDICES AND REFERENCE DOCUMENTS

Document Control

- **Document Title:** Backup Policy Appendices and Reference Documents (NIST Framework Aligned)
- **Document Number:** ACME-IT-POL-001-APP
- **Version:** 2.0
- **Effective Date:** January 2025
- **Classification:** Internal Use Only
- **Parent Document:** ACME-IT-POL-001 Data Backup and Recovery Policy

---

APPENDIX A: CRITICAL APPLICATION INVENTORY (NIST SP 800-60 CATEGORIZED)

A.1 Mission-Essential Functions (Tier 1) - HIGH Impact Systems

A.1.1 SAP ERP System

- **Application ID:** APP-001
- **System Name:** SAP S/4HANA Enterprise Resource Planning
- **NIST Categorization:** HIGH/HIGH/HIGH (Confidentiality/Integrity/Availability)
- **Business Function:** Financial management, procurement, inventory control
- **Technical Specifications:**
  - **Database:** SAP HANA 2.0 (12TB primary database)

- **Operating System:** SUSE Linux Enterprise Server 15 SP4
- **Servers:** 8 application servers, 4 database servers (HANA System Replication)
- **Location:** Sydney Primary Data Center (Tier III)
- **DR Location:** Melbourne Secondary Data Center (Tier III)
- **Cloud Backup:** Azure Australia East region

- **Recovery Requirements (NIST CP-10):**
  - **RTO:** 2 hours | **RPO:** 15 minutes
  - **Backup Method:** HANA System Replication + hourly snapshots with NIST CP-9 compliance
  - **Retention:** 7 years (financial compliance), 3 years (operational data)
  - **Validation:** Daily automated backup verification (NIST CP-9(7))
- **Dependencies:** Inventory Management, Customer Loyalty Platform
- **Business Impact:** Critical - All financial operations cease, regulatory compliance at risk
- **DR Manager Escalation:** Category 1 incident - immediate CIO notification required

A.1.2 Oracle POS System

- **Application ID:** APP-002
- **System Name:** Oracle Retail Point-of-Service (ORPOS)
- **NIST Categorization:** HIGH/HIGH/HIGH (Customer transaction processing)
- **Business Function:** In-store transaction processing across 450+ retail locations
- **Technical Specifications:**
  - **Database:** Oracle Database 19c RAC (8TB)
  - **Operating System:** Oracle Linux 8.6
  - **Servers:** 12 application servers, 6 database nodes (Active-Active cluster)

0

- **Location:** Sydney Primary + Melbourne Secondary (load balanced)
- **Store Integration:** Real-time synchronization to 450+ store locations
- **Network:** Dedicated MPLS with 10Gbps inter-site connectivity

- **Recovery Requirements (NIST CP-10):**
  - **RTO:** 1 hour | **RPO:** 5 minutes
  - **Backup Method:** Oracle Data Guard + continuous log shipping
  - **Retention:** 7 years (transaction records for audit compliance)
  - **Validation:** Real-time replication monitoring with automated failover testing
- **Dependencies:** Customer Loyalty Platform, Financial Reporting System
- **Business Impact:** Critical - Immediate revenue loss, customer service disruption
- **DR Manager Notes:** Highest priority for recovery - affects all 450+ stores simultaneously

A.1.3 Customer Loyalty Platform

- **Application ID:** APP-003
- **System Name:** ACME Rewards Customer Management System
- **NIST Categorization:** HIGH/HIGH/MODERATE (Customer personal data)
- **Business Function:** Customer loyalty program, personalization, promotional campaigns
- **Technical Specifications:**
  - **Database:** Microsoft SQL Server 2022 Always On Availability Groups (4TB)
  - **Operating System:** Windows Server 2022 Datacenter
  - **Servers:** 6 application servers, 4 database servers (Always On cluster)
  - **Location:** Sydney Primary Data Center with Melbourne replica
  - **Integration:** Mobile app (iOS/Android), POS systems, marketing automation

- **APIs:** RESTful services with OAuth 2.0 authentication

- **Recovery Requirements (NIST CP-10):**
  - **RTO:** 2 hours | **RPO:** 15 minutes
  - **Backup Method:** Always On Availability Groups + log shipping to cloud
  - **Retention:** 5 years (customer analytics), permanent (legal holds)
  - **Privacy Compliance:** Australian Privacy Act, APP 11 security requirements
- **Dependencies:** POS System, Marketing Automation Platform
- **Business Impact:** High - Customer experience degradation, lost personalization data
- **DR Manager Focus:** Customer data protection priority, privacy breach risk

A.1.4 Inventory Management System

- **Application ID:** APP-004
- **System Name:** ACME Intelligent Inventory Management (AIIM)
- **NIST Categorization:** HIGH/HIGH/HIGH (Supply chain critical)
- **Business Function:** Stock control, automated ordering, supply chain optimization
- **Technical Specifications:**
  - **Database:** MySQL 8.0 with Galera Cluster (6TB)
  - **Operating System:** Ubuntu Server 22.04 LTS
  - **Servers:** 10 application servers, 6 database servers (multi-master replication)
  - **Location:** Sydney Primary + Melbourne Secondary (active-active)
  - **Integration:** SAP ERP, 200+ supplier systems, IoT sensors (12,000+ devices)
  - **Analytics:** Real-time inventory optimization with machine learning
- **Recovery Requirements (NIST CP-10):**

- **RTO:** 2 hours | **RPO:** 15 minutes
  - **Backup Method:** Galera cluster replication + incremental backups to AWS S3
  - **Retention:** 3 years (inventory movements), 7 years (financial impacts)
  - **Validation:** Hourly consistency checks across cluster nodes
- **Dependencies:** SAP ERP, Supplier portals, IoT sensor network
- **Business Impact:** Critical - Stock-outs, over-ordering, $2M+ daily supply chain impact
- **DR Manager Priority:** Supply chain disruption affects 450+ stores within 24 hours

A.1.5 Financial Reporting System

- **Application ID:** APP-005
- **System Name:** ACME Financial Intelligence Platform (AFIP)
- **NIST Categorization:** HIGH/HIGH/MODERATE (Financial reporting & compliance)
- **Business Function:** Financial reporting, regulatory compliance, business intelligence
- **Technical Specifications:**
  - **Database:** Microsoft SQL Server 2022 with Analysis Services (5TB)
  - **Operating System:** Windows Server 2022 Standard
  - **Servers:** 4 application servers, 4 database servers, 2 SSAS cubes
  - **Location:** Sydney Primary Data Center (secure financial zone)
  - **Integration:** SAP ERP, external audit systems (Big 4 accounting firm)
  - **Reporting:** Power BI Premium, SSRS, regulatory submission automation
- **Recovery Requirements (NIST CP-10):**
  - **RTO:** 2 hours | **RPO:** 15 minutes
  - **Backup Method:** Always On Availability Groups + cube backups + cloud archive

0

- **Retention:** 7 years (financial reports), permanent (annual reports, audit)
- **Compliance:** ASX reporting requirements, ASIC regulatory obligations

- **Dependencies:** SAP ERP, external audit systems, regulatory reporting APIs
- **Business Impact:** Critical - Regulatory non-compliance, ASX reporting failures
- **DR Manager Notes:** Regulatory timeline compliance critical - ASIC penalties apply

A.2 Primary Business Functions (Tier 2) - MODERATE Impact Systems

A.2.1 Supply Chain Management (APP-006)

- **System:** ACME Supply Chain Orchestrator (ASCO)
- **NIST Categorization:** MODERATE/HIGH/MODERATE
- **Function:** Supplier management, logistics coordination, delivery scheduling
- **Recovery:** RTO 4 hours / RPO 1 hour
- **Critical Dependencies:** 200+ supplier integrations, logistics partners

A.2.2 Human Resources Information System (APP-007)

- **System:** Workday HCM Enterprise (SaaS)
- **NIST Categorization:** HIGH/HIGH/MODERATE (Employee PII)
- **Function:** Employee management, payroll (5,000+ employees), performance tracking
- **Recovery:** RTO 4 hours / RPO 4 hours
- **Compliance:** Fair Work Act, superannuation obligations

A.2.3 Customer Service Portal (APP-008)

- **System:** Salesforce Service Cloud
- **NIST Categorization:** MODERATE/HIGH/MODERATE

- **Function:** Customer support, case management, knowledge base
- **Recovery:** RTO 8 hours / RPO 4 hours
- **Integration:** POS systems, Customer Loyalty Platform

A.2.4 Email and Collaboration Platform (APP-009)

- **System:** Microsoft 365 Enterprise E5
- **NIST Categorization:** MODERATE/MODERATE/MODERATE
- **Function:** Email, SharePoint, Teams, OneDrive
- **Recovery:** RTO 8 hours / RPO 4 hours
- **Users:** 5,000+ employees, 450+ store locations

A.2.5 Marketing Automation Platform (APP-010)

- **System:** Adobe Campaign + Marketo Engage
- **NIST Categorization:** MODERATE/MODERATE/LOW
- **Function:** Email marketing, campaign management, customer segmentation
- **Recovery:** RTO 8 hours / RPO 4 hours
- **Integration:** Customer Loyalty Platform, analytics systems

A.2.6 Business Intelligence and Analytics (APP-011)

- **System:** Tableau Server + Power BI Premium
- **NIST Categorization:** MODERATE/HIGH/MODERATE
- **Function:** Data visualization, executive dashboards, self-service analytics
- **Recovery:** RTO 8 hours / RPO 4 hours
- **Data Sources:** All Tier 1 systems, external market data

A.2.7 Security and Surveillance Systems (APP-012)

- **System:** Milestone XProtect + Genetec Security Center
- **NIST Categorization:** MODERATE/HIGH/MODERATE
- **Function:** Video surveillance (450+ stores), access control, incident management
- **Recovery:** RTO 8 hours / RPO 4 hours
- **Storage:** 90-day retention, 24/7 monitoring

A.3 Supporting Business Functions (Tier 3) - LOW Impact Systems

A.3.1 Document Management System (APP-013)

- **System:** SharePoint Server 2022 + Microsoft Purview
- **Function:** Document storage, version control, workflow management
- **Recovery:** RTO 24 hours / RPO 24 hours

A.3.2 Training and Learning Management (APP-014)

- **System:** Cornerstone OnDemand LMS
- **Function:** Employee training, compliance tracking, certification management
- **Recovery:** RTO 24 hours / RPO 24 hours

A.3.3 Facility Management System (APP-015)

- **System:** IBM TRIRIGA + Archibus
- **Function:** Space management, maintenance scheduling, energy monitoring
- **Recovery:** RTO 24 hours / RPO 24 hours

A.3.4 Vehicle Fleet Management (APP-016)

- **System:** Verizon Connect Fleet Management
- **Function:** Vehicle tracking, maintenance scheduling, driver management
- **Recovery:** RTO 24 hours / RPO 24 hours

A.3.5 Energy Management System (APP-017)

- **System:** Schneider Electric EcoStruxure
- **Function:** Energy monitoring, sustainability reporting, cost optimization
- **Recovery:** RTO 24 hours / RPO 24 hours

A.3.6 Employee Self-Service Portal (APP-018)

- **System:** Custom .NET application + SQL Server
- **Function:** Employee portal, time tracking, benefits management
- **Recovery:** RTO 24 hours / RPO 24 hours

A.3.7 Vendor Portal and Procurement (APP-019)

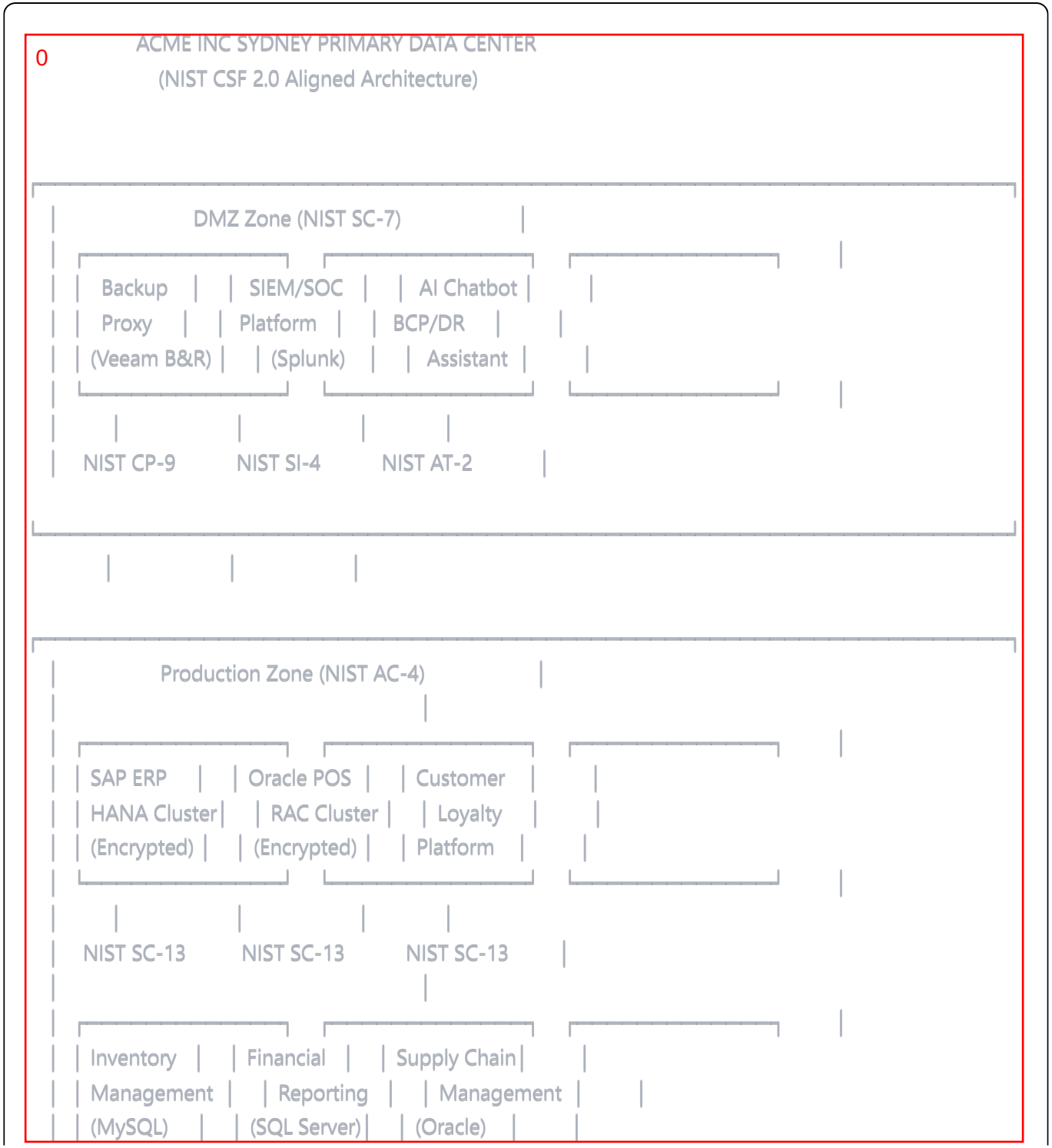
- **System:** SAP Ariba + Oracle Supplier Network
- **Function:** Supplier onboarding, procurement processes, contract management
- **Recovery:** RTO 8 hours / RPO 4 hours

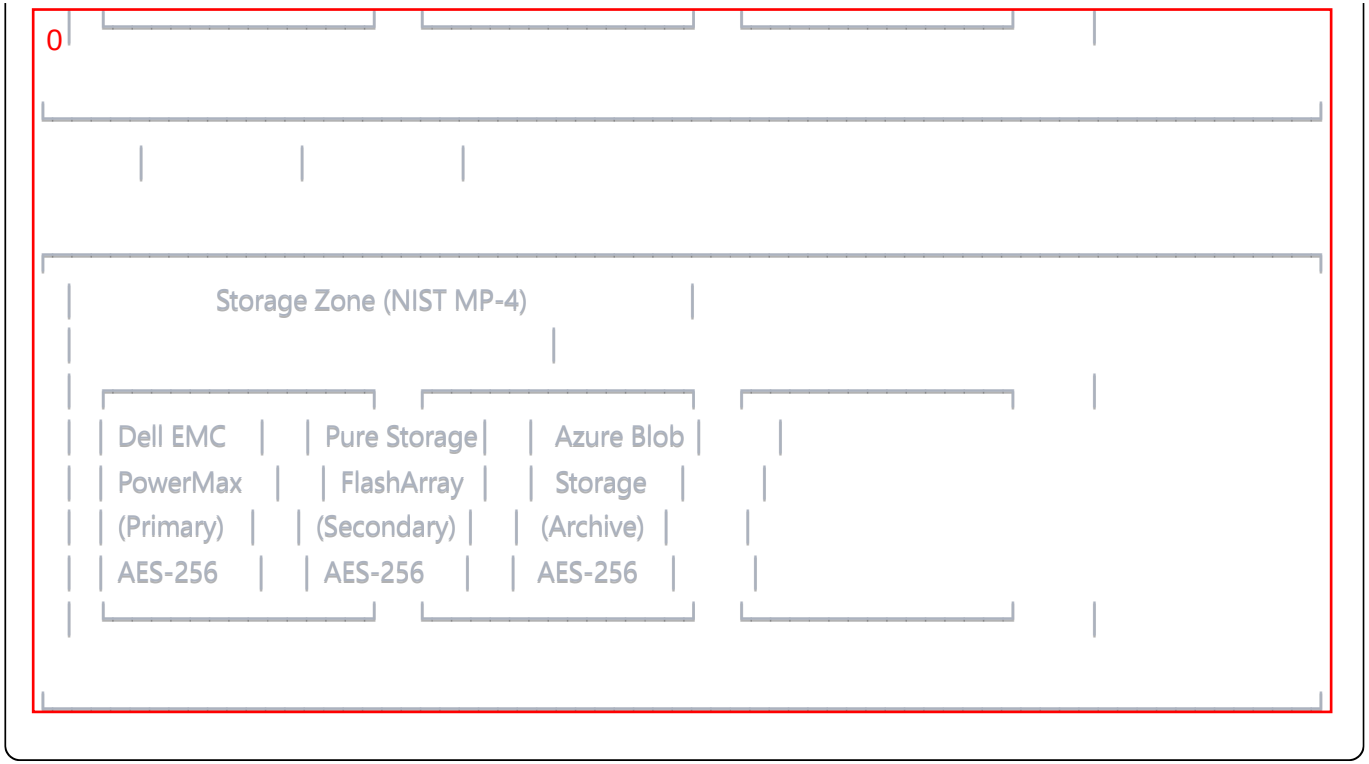
A.3.8 Quality Management System (APP-020)

- **System:** SAP Quality Management + TrackWise
- **Function:** Quality control, compliance tracking, audit management
- **Recovery:** RTO 24 hours / RPO 24 hours

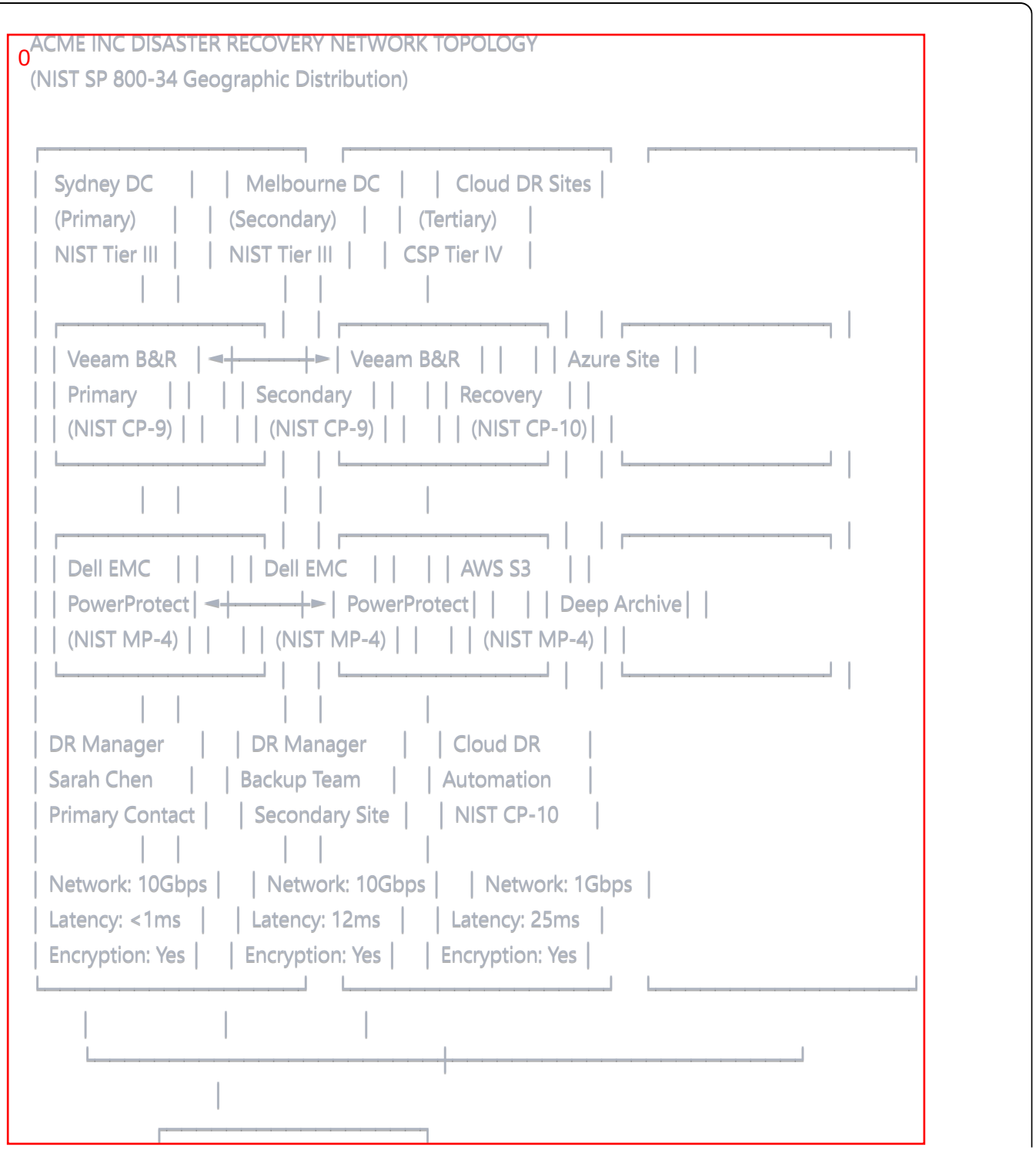
APPENDIX B: NETWORK TOPOLOGY DIAGRAMS (NIST SP 800-53 SECURITY ARCHITECTURE)

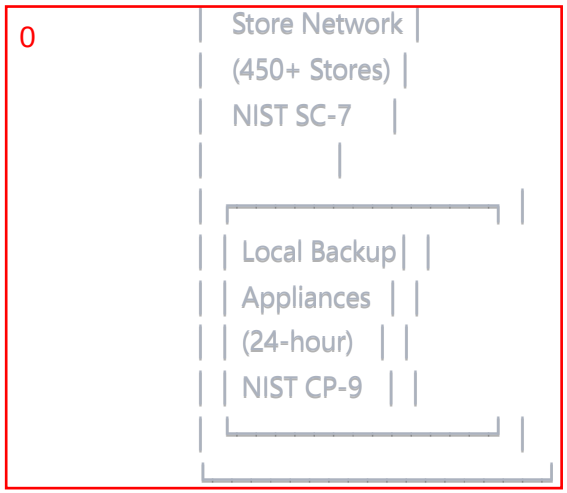
B.1 NIST Cybersecurity Framework Backup Network Architecture


0
ACME INC SYDNEY PRIMARY DATA CENTER
(NIST CSF 2.0 Aligned Architecture)
DMZ Zone (NIST SC-7)
Backup Proxy (Veeam B&R)
SIEM/SOC Platform (Splunk)
AI Chatbot BCP/DR Assistant
NIST CP-9
NIST SI-4
NIST AT-2
Production Zone (NIST AC-4)
SAP ERP HANA Cluster (Encrypted)
Oracle POS RAC Cluster (Encrypted)
Customer Loyalty Platform
NIST SC-13
NIST SC-13
NIST SC-13
Inventory Management (MySQL)
Financial Reporting (SQL Server)
Supply Chain Management (Oracle)

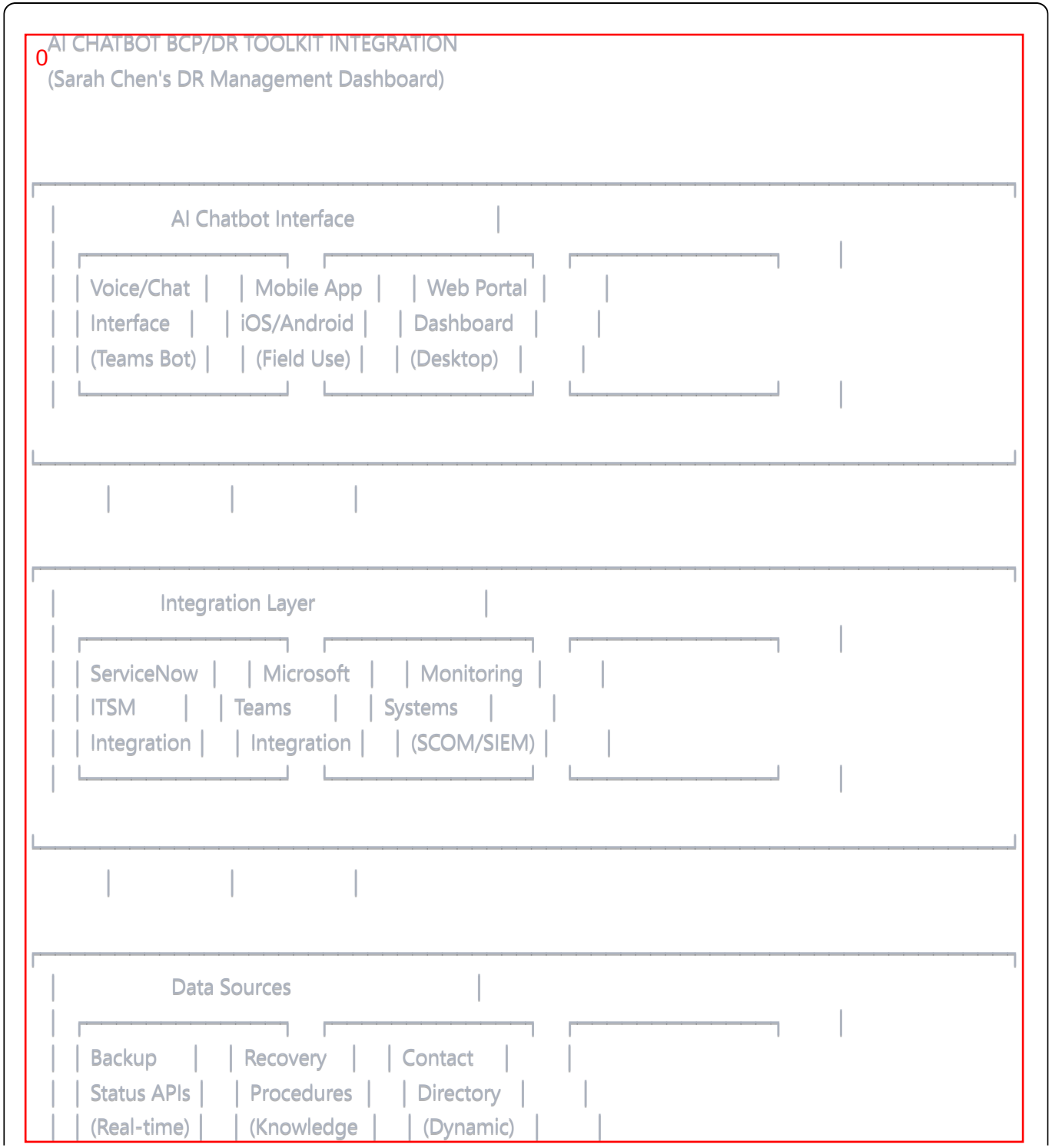


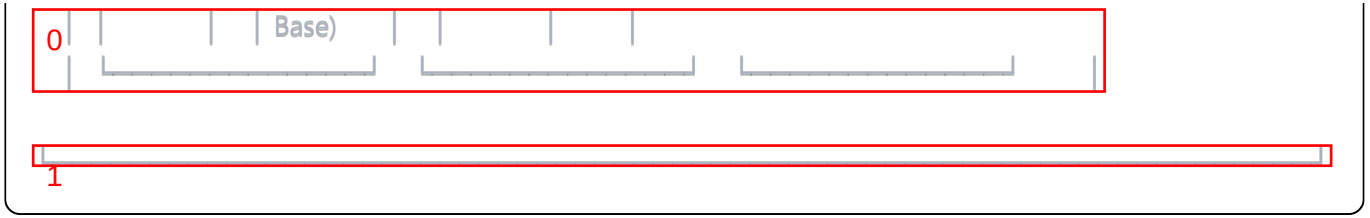
B.2 Multi-Site Disaster Recovery Network (NIST CP-6/CP-7)


ACME INC DISASTER RECOVERY NETWORK TOPOLOGY
(NIST SP 800-34 Geographic Distribution)
Sydney DC
(Primary)
NIST Tier III
Melbourne DC
(Secondary)
NIST Tier III
Cloud DR Sites
(Tertiary)
CSP Tier IV
Veeam B&R
Primary
(NIST CP-9)
Veeam B&R
Secondary
(NIST CP-9)
Azure Site
Recovery
(NIST CP-10)
Dell EMC
PowerProtect
(NIST MP-4)
Dell EMC
PowerProtect
(NIST MP-4)
AWS S3
Deep Archive
(NIST MP-4)
DR Manager
Sarah Chen
Primary Contact
DR Manager
Backup Team
Secondary Site
Cloud DR
Automation
NIST CP-10
Network: 10Gbps
Latency: <1ms
Encryption: Yes
Network: 10Gbps
Latency: 12ms
Encryption: Yes
Network: 1Gbps
Latency: 25ms
Encryption: Yes



B.3 AI Chatbot Integration Architecture for DR Manager


AI CHATBOT BCP/DR TOOLKIT INTEGRATION
(Sarah Chen's DR Management Dashboard)
AI Chatbot Interface
Voice/Chat Interface (Teams Bot)
Mobile App iOS/Android (Field Use)
Web Portal Dashboard (Desktop)
Integration Layer
ServiceNow ITSM Integration
Microsoft Teams Integration
Monitoring Systems (SCOM/SIEM)
Data Sources
Backup Status APIs (Real-time)
Recovery Procedures (Knowledge
Contact Directory (Dynamic)



B.4 Network Security Controls (NIST SP 800-53)

Network Segment	NIST Controls	Security Measures
DMZ Zone	SC-7, AC-4	Firewall rules, IPS, network segmentation
Production Zone	SC-7, SC-8	Encrypted communication, access controls
Storage Zone	MP-4, SC-13	Encryption at rest, secure key management
Management Network	AC-2, AU-2	MFA required, full audit logging
WAN Connections	SC-8, SC-12	VPN encryption, certificate management

---

APPENDIX C: EMERGENCY CONTACT LIST (DR MANAGER FOCUSED)

C.1 DR Manager Primary Contacts (Sarah Chen's Team)

C.1.1 DR Manager - Primary Contact

Role	Name	Mobile	Email	Backup
DR Manager	**Sarah Chen**	**+61 404 XXX 001**	**s.chen@acme.com.au**	**IT Operations Manager**
Certifications	CBCP, PMP	Location	Sydney HQ	Escalation
Responsibilities	Overall DR coordination, vendor management, executive reporting			
Availability	24/7 on-call rotation	Backup Phone	+61 404 XXX 002	

C.1.2 DR Specialists Team (Sarah's Direct Reports)

Role	Name	Mobile	Email	Specialization
Senior DR Analyst	Michael Rodriguez	+61 404 XXX 010	m.rodriguez@acme.com.au	Database Recovery
DR Systems Engineer	Jennifer Walsh	+61 404 XXX 011	j.walsh@acme.com.au	Infrastructure/Cloud
DR Compliance Lead	David Kumar	+61 404 XXX 012	d.kumar@acme.com.au	NIST/ISO Compliance
DR Communications	Lisa Chang	+61 404 XXX 013	l.chang@acme.com.au	Stakeholder Comms
DR Testing Lead	Mark Peterson	+61 404 XXX 014	m.peterson@acme.com.au	Validation/Testing
Store DR Coordinator	Rachel Kim	+61 404 XXX 015	r.kim@acme.com.au	Retail Operations

C.2 Executive Escalation Chain (Category 1 Incidents)

C.2.1 Immediate Escalation (Within 15 minutes)

Role	Name	Mobile	Email	Escalation Trigger
CISO	Amanda Foster	+61 404 XXX 020	a.foster@acme.com.au	Security-related DR events
CIO	Robert Taylor	+61 404 XXX 021	r.taylor@acme.com.au	All Category 1 incidents
COO	Catherine Brown	+61 404 XXX 022	c.brown@acme.com.au	Store operations impact

C.2.2 Executive Team (Within 30 minutes)

Role	Name	Mobile	Email	Notification Type
CEO	Sarah Johnson	+61 404 XXX 030	s.johnson@acme.com.au	Category 1 incidents
CFO	David Williams	+61 404 XXX 031	d.williams@acme.com.au	Financial system impacts
Chief Legal	Michelle Wong	+61 404 XXX 032	m.wong@acme.com.au	Regulatory/privacy breaches

C.3 Technical Teams (On-Call Rotation)

C.3.1 Database Administration Team

Week	Primary DBA	Secondary DBA	Specialty
Week 1	Tom Anderson +61 404 XXX 040	Jenny Lee +61 404 XXX 041	Oracle/SAP HANA
Week 2	Sarah Davis +61 404 XXX 042	Peter Kim +61 404 XXX 043	SQL Server/MySQL
Week 3	Andrew Clarke +61 404 XXX 044	Linda Zhang +61 404 XXX 045	Oracle/NoSQL
Week 4	Kevin O'Brien +61 404 XXX 046	Emma Johnson +61 404 XXX 047	SQL Server/Cloud

C.3.2 Infrastructure Team

Week	Primary SysAdmin	Secondary SysAdmin	Specialty
Week 1	Daniel Garcia +61 404 XXX 050	Sophie Mitchell +61 404 XXX 051	VMware/Windows
Week 2	Ryan Clarke +61 404 XXX 052	Alice Chen +61 404 XXX 053	Linux/Cloud
Week 3	Patrick O'Connor +61 404 XXX 054	Steve Morrison +61 404 XXX 055	Network/Security
Week 4	Anthony Rodriguez +61 404 XXX 056	Helen Mitchell +61 404 XXX 057	Storage/Backup

C.4 Business Stakeholder Contacts

C.4.1 Store Operations (450+ Stores)

Region	Regional Manager	Mobile	Email	Stores Count
NSW/ACT	Christopher Evans	+61 404 XXX 060	c.evans@acme.com.au	180 stores
VIC/TAS	Susan Campbell	+61 404 XXX 061	s.campbell@acme.com.au	145 stores
QLD/NT	James Wilson	+61 404 XXX 062	j.wilson@acme.com.au	85 stores
WA/SA	Catherine Brown	+61 404 XXX 063	c.brown@acme.com.au	40 stores

C.4.2 Key Business Functions

Function	Manager	Mobile	Email	DR Impact
Finance	Financial Controller	+61 404 XXX 070	finance@acme.com.au	SAP ERP, Financial Reporting
Supply Chain	Supply Chain Director	+61 404 XXX 071	supply@acme.com.au	Inventory, Procurement
Customer Service	Customer Service Manager	+61 404 XXX 072	service@acme.com.au	Customer Portal, Loyalty
Marketing	Marketing Director	+61 404 XXX 073	marketing@acme.com.au	Marketing Automation

C.5 AI Chatbot Integration Contacts

C.5.1 AI Chatbot Support Team

Role	Contact	Phone	Email	Availability
AI Solutions Architect	Dr. Alex Thompson	+61 404 XXX 080	a.thompson@acme.com.au	Business hours
Chatbot Administrator	Priya Sharma	+61 404 XXX 081	p.sharma@acme.com.au	24/7 support
Integration Specialist	Marcus Johnson	+61 404 XXX 082	m.johnson@acme.com.au	Business hours

C.5.2 ServiceNow Integration

Role	Contact	Phone	Email	Specialty
ServiceNow Admin	Jennifer Walsh	+61 404 XXX 090	j.walsh@acme.com.au	ITSM Integration
Workflow Designer	David Kumar	+61 404 XXX 091	d.kumar@acme.com.au	Automation

APPENDIX D: VENDOR CONTACT INFORMATION (NIST SA-9 COMPLIANT)

D.1 Primary Technology Vendors (24/7 Support)

D.1.1 Microsoft Corporation (Azure, Office 365)

Service Level	Contact Type	Phone	Email	Response Time
Premier Support	Enterprise	+61 1800 197 503	premier@microsoft.com	1 hour
Azure Critical	Priority 1	+61 1800 197 503	azuresupport@microsoft.com	15 minutes
Security Response	MSRC	+1 425 882 8080	secure@microsoft.com	Immediate

Sarah Chen's Account Team:

- **Customer Success Manager:** Jennifer Walsh - +61 404 XXX 100 - j.walsh@microsoft.com
- **Technical Account Manager:** David Kumar - +61 404 XXX 101 - d.kumar@microsoft.com
- **Premier Support Engineer:** Lisa Chang - +61 404 XXX 102 - l.chang@microsoft.com
- **DR Specialist:** Mark Peterson - +61 404 XXX 103 - m.peterson@microsoft.com

NIST Compliance: Microsoft SOC 2 Type II, FedRAMP High, ISO 27001

D.1.2 Amazon Web Services (AWS)

Service Level	Contact Type	Phone	Email	Response Time
Enterprise Support	Technical Account Manager	+61 1800 751 575	enterprise@aws.com	15 minutes
Business Support	General Support	+61 1800 751 575	aws-support@amazon.com	1 hour
Security Team	AWS Security	+1 206 266 4064	aws-security@amazon.com	15 minutes

Account Team:

- **Technical Account Manager:** Rachel Kim - +61 404 XXX 110 - r.kim@amazon.com
- **Solutions Architect:** Steve Morrison - +61 404 XXX 111 - s.morrison@amazon.com
- **DR Consultant:** Alice Chen - +61 404 XXX 112 - a.chen@amazon.com

NIST Compliance: AWS FedRAMP High, SOC 1/2/3, ISO 27001

D.1.3 Dell Technologies (Infrastructure)

Service Level	Contact Type	Phone	Email	Response Time
ProSupport Plus	Critical Hardware	1800 624 253	prosupport@dell.com	4-hour onsite
Premium Support	Software/Firmware	1800 624 253	premium@dell.com	1 hour
Mission Critical	Emergency Response	1800 624 253	mission-critical@dell.com	2-hour onsite

Account Team for Sarah Chen:

- **Enterprise Account Executive:** Patrick O'Connor - +61 404 XXX 120 - p.oconnor@dell.com
- **Technical Account Manager:** Sophie Mitchell - +61 404 XXX 121 - s.mitchell@dell.com

- **DR Hardware Specialist:** Anthony Rodriguez - +61 404 XXX 122 - a.rodriguez@dell.com

NIST Compliance: ISO 27001, SOC 2 Type II

D.1.4 Veeam Software (Backup & Replication)

Service Level	Contact Type	Phone	Email	Response Time
Premier Support	24x7 Technical	+61 1800 441 953	support@veeam.com	1 hour
Emergency Support	Critical Issues	+61 1800 441 953	emergency@veeam.com	30 minutes
Professional Services	DR Consulting	+61 2 8218 2550	services@veeam.com	4 hours

Dedicated Support for DR Operations:

- **Customer Success Manager:** Helen Mitchell - +61 404 XXX 130 - h.mitchell@veeam.com
- **Senior Support Engineer:** Christopher Evans - +61 404 XXX 131 - c.evans@veeam.com
- **DR Architect:** Susan Campbell - +61 404 XXX 132 - s.campbell@veeam.com

D.2 Database Vendors (Mission-Critical Support)

D.2.1 Oracle Corporation

Service Level	Contact Type	Phone	Email	Response Time
Premier Support	Database Critical	1800 555 815	oracle.support@oracle.com	1 hour
Security Response	Security Patches	1800 555 815	security-alert@oracle.com	15 minutes
RAC Support	Cluster Specialists	1800 555 815	rac-support@oracle.com	30 minutes

DR-Focused Support Team:

- **Account Manager:** James Wilson - +61 404 XXX 140 - j.wilson@oracle.com
- **RAC Specialist:** Catherine Brown - +61 404 XXX 141 - c.brown@oracle.com

D.2.2 SAP Australia

Service Level	Contact Type	Phone	Email	Response Time
Enterprise Support	SAP BASIS/HANA	1800 308 855	support@sap.com	1 hour
HANA Premium	In-Memory DB	1800 308 855	hana-support@sap.com	30 minutes
Mission Critical	Emergency Response	1800 308 855	mission-critical@sap.com	15 minutes

Key Contacts:

- **Customer Success Partner:** Daniel Garcia - +61 404 XXX 150 - d.garcia@sap.com
- **HANA Architect:** Sophie Mitchell - +61 404 XXX 151 - s.mitchell@sap.com

D.3 Cloud Application Vendors

D.3.1 Salesforce (Customer Service Platform)

Service Level	Contact Type	Phone	Email	Response Time
Premier Support	24x7 Technical	+61 1800 667 638	premier@salesforce.com	1 hour
Mission Critical	P1 Issues	+61 1800 667 638	critical@salesforce.com	30 minutes

D.3.2 Workday (HR Systems)

Service Level	Contact Type	Phone	Email	Response Time
Premium Support	HR Systems	+61 2 8224 8200	support@workday.com	2 hours
Emergency Support	Payroll Critical	+61 2 8224 8200	emergency@workday.com	1 hour

D.4 AI Chatbot Technology Partners

D.4.1 Microsoft (Teams Bot Integration)

Service	Contact Type	Phone	Email	Availability
Bot Framework Support	Developer Support	+61 1800 197 503	botframework@microsoft.com	Business hours
Cognitive Services	AI Platform	+61 1800 197 503	cognitive@microsoft.com	24x7

D.4.2 OpenAI (GPT Integration)

Service	Contact Type	Phone	Email	Availability
Enterprise API	Technical Support	+1 415 555 0199	enterprise@openai.com	Business hours
Safety & Security	Security Team	+1 415 555 0199	safety@openai.com	24x7

D.5 Telecommunications & Connectivity

D.5.1 Telstra Corporation (Primary WAN Provider)

Service	Contact Type	Phone	Email	Response Time
Enterprise NOC	Network Operations	132 200	noc@telstra.com	24x7
Account Management	Enterprise Team	132 200	enterprise@telstra.com	Business hours
Emergency Response	Critical Outages	000	emergency@telstra.com	Immediate

Sarah Chen's Account Team:

- **Enterprise Account Manager:** Ryan Clarke - +61 404 XXX 160 - r.clarke@telstra.com
- **Network Architect:** Alice Chen - +61 404 XXX 161 - a.chen@telstra.com
- **NOC Escalation Contact:** Patrick O'Connor - +61 404 XXX 162 - p.oconnor@telstra.com

---

APPENDIX E: NIST CONTROLS MAPPING MATRIX

E.1 NIST SP 800-53 Rev 5 Controls Implementation

Control Family	Control ID	Control Name	ACME Implementation	Policy Section	Validation Method
Access Control (AC)	AC-2	Account Management	Role-based backup access with MFA	Section 6.2	Quarterly access reviews
Access Control (AC)	AC-4	Information Flow Enforcement	Network segmentation for backup traffic	Section 5.1.2	Monthly network audits
Access Control (AC)	AC-6	Least Privilege	Minimal backup operator permissions	Section 6.2	Semi-annual privilege reviews
Audit and Accountability (AU)	AU-2	Event Logging	All backup/restore activities logged	Section 12.3	Daily log analysis
Audit and Accountability (AU)	AU-3	Content of Audit Records	Detailed audit trail with timestamps	Section 12.3	Weekly audit verification
Audit and Accountability (AU)	AU-4	Audit Log Storage Capacity	7-year audit log retention	Section 12.3	Monthly capacity monitoring
Audit and Accountability (AU)	AU-6	Audit Record Review	Regular log review for anomalies	Section 12.3	Daily automated analysis
Audit and Accountability (AU)	AU-9	Protection of Audit Information	Encrypted and tamper-proof logs	Section 12.3	Quarterly integrity checks
Contingency Planning (CP)	CP-2	Contingency Plan	Comprehensive backup and DR policy	Section 1	Annual plan review

Control Family	Control ID	Control Name	ACME Implementation	Policy Section	Validation Method
Contingency Planning (CP)	CP-4	Contingency Plan Testing	Monthly, quarterly, and annual testing	Section 9	Test result documentation
Contingency Planning (CP)	CP-6	Alternate Storage Site	Geographic distribution of backups	Section 5.1.2	Quarterly site verification
Contingency Planning (CP)	CP-7	Alternate Processing Site	Melbourne secondary data center	Section 5.1.2	Semi-annual DR testing
Contingency Planning (CP)	CP-9	Information System Backup	Comprehensive backup procedures	Section 5.2	Daily backup verification
Contingency Planning (CP)	CP-10	Information System Recovery	Detailed recovery procedures	Section 11.2	Monthly recovery testing

E.2 NIST Cybersecurity Framework 2.0 Implementation

Function	Category	Subcategory	ACME Implementation	Responsible Party	Measurement
GOVERN (GV)	GV.OC	Organizational Cybersecurity Strategy	Executive oversight of backup strategy	CIO, DR Manager	Quarterly reviews
GOVERN (GV)	GV.RM	Risk Management Strategy	Risk-based backup classification	DR Manager, Security	Annual risk assessment
IDENTIFY (ID)	ID.AM	Asset Management	Critical application inventory	DR Manager, IT Teams	Monthly inventory updates
IDENTIFY (ID)	ID.RA	Risk Assessment	Business impact analysis for systems	DR Manager, Business	Annual BIA updates
PROTECT (PR)	PR.AC	Identity Management and Access Control	Multi-factor authentication for backup systems	Security Team	Monthly access audits
PROTECT (PR)	PR.DS	Data Security	Encryption of all backup data	Security, DR Teams	Daily encryption verification
PROTECT (PR)	PR.IP	Information Protection Processes	Backup procedures and documentation	DR Manager	Quarterly procedure review
PROTECT (PR)	PR.MA	Maintenance	Regular backup system maintenance	IT Operations	Weekly maintenance logs
PROTECT (PR)	PR.PT	Protective Technology	Backup software and infrastructure	DR Manager, IT Ops	Monthly performance monitoring
DETECT (DE)	DE.AE	Anomalies and Events	Backup failure detection and alerting	DR Manager, Monitoring	Real-time monitoring

Function	Category	Subcategory	ACME Implementation	Responsible Party	Measurement
DETECT (DE)	DE.CM	Security Continuous Monitoring	SIEM integration for backup systems	Security, DR Teams	24x7 monitoring
RESPOND (RS)	RS.RP	Response Planning	Incident response procedures	DR Manager	Quarterly tabletop exercises
RESPOND (RS)	RS.CO	Communications	Stakeholder notification procedures	DR Manager, Comms	Monthly communication tests
RESPOND (RS)	RS.AN	Analysis	Incident analysis and forensics	Security, DR Teams	Post-incident reviews
RESPOND (RS)	RS.MI	Mitigation	Incident containment procedures	DR Manager, IT Ops	Incident response exercises
RESPOND (RS)	RS.IM	Improvements	Lessons learned integration	DR Manager	Quarterly improvement reviews
RECOVER (RC)	RC.RP	Recovery Planning	Comprehensive recovery procedures	DR Manager	Monthly recovery testing
RECOVER (RC)	RC.IM	Recovery Plan Implementation	Execution of recovery procedures	DR Manager, IT Teams	Recovery exercise validation
RECOVER (RC)	RC.CO	Recovery Communications	Stakeholder updates during recovery	DR Manager, Comms	Communication plan testing

E.3 ISO 27001:2022 Annex A Controls Mapping

Control	Control Title	ACME Implementation	Evidence Required
A.5.2	Information security roles and responsibilities	Defined DR team roles and responsibilities	Role documentation, training records
A.5.7	Threat intelligence	Integration with security monitoring	Threat intelligence reports
A.8.9	Access management	Role-based access for backup systems	Access control matrix, audit logs
A.8.10	Information in processing systems	Data classification and handling	Data classification procedures
A.8.24	Use of cryptography	Encryption of backup data	Encryption verification reports
A.12.3	Information backup	Comprehensive backup procedures	Backup policy, test results
A.17.1	Information security continuity	Business continuity planning	BCP documentation, test results
A.17.2	Redundancies	Geographic distribution of backups	Site verification, failover tests

E.4 Australian Privacy Principles (APP) Compliance

APP	Principle	ACME Implementation	Validation Method
APP 1	Open and transparent privacy policy	Customer data backup transparency	Privacy policy updates
APP 3	Collection of solicited personal information	Data classification in backups	Collection notices
APP 5	Notification of collection	Backup data inclusion notices	Documentation review
APP 6	Use or disclosure	Backup access controls	Access audit reports
APP 8	Cross-border disclosure	Australian data residency	Location verification
APP 10	Quality of personal information	Data integrity in backups	Quality assurance tests
APP 11	Security of personal information	Encryption and access controls	Security assessments
APP 12	Access to personal information	Backup data access procedures	Access request logs
APP 13	Correction of personal information	Data correction in backups	Correction procedures

APPENDIX F: RECOVERY PROCEDURE CHECKLISTS (NIST CP-10 ALIGNED)

F.1 AI Chatbot-Enabled Recovery Procedures (Sarah Chen's Toolkit)

F.1.1 AI Chatbot Integration for DR Operations

Voice Commands for DR Manager:

- "What's the status of SAP backup recovery?" - Real-time status updates

- "Walk me through Oracle POS recovery steps" - Step-by-step guidance
- "Who's the on-call DBA for emergency escalation?" - Contact information
- "Generate Category 1 incident report for executive briefing" - Automated reporting
- "Schedule DR test for Customer Loyalty Platform" - Test coordination

Automated Workflows Triggered by Chatbot:

1. **Incident Declaration:** "Declare Category 1 incident for SAP ERP failure"
2. **Team Assembly:** Automatic notification of DR specialists
3. **Status Updates:** Real-time updates to executive team
4. **Documentation:** Auto-generation of incident timeline
5. **Post-Recovery:** Automated lessons learned compilation

F.1.2 Category 1 Incident Response (Critical Systems)

Phase 1: Immediate Response (0-15 minutes) - NIST IR-4

- ☐ **AI Chatbot Activation:** "Initiate Category 1 DR response for [System Name]"
- ☐ Automatic escalation to Sarah Chen (DR Manager)
- ☐ Notification to on-call technical teams
- ☐ Executive team alert (CIO, CISO, COO)
- ☐ ServiceNow incident ticket creation
- ☐ **Initial Assessment (NIST CP-4)**
- ☐ AI Chatbot queries: "What systems are affected?"
- ☐ Business impact assessment: "What's the revenue impact?"
- ☐ Customer impact evaluation: "How many stores affected?"
- ☐ Recovery time estimation: "What's our expected RTO?"

Phase 2: Recovery Coordination (15-60 minutes) - NIST CP-10

- [ ] **Recovery Team Assembly**
- [ ] AI Chatbot: "Assemble DR team for [System Name] recovery"
- [ ] Technical specialists notification
- [ ] Business stakeholder communication
- [ ] Vendor escalation if required
- [ ] **Recovery Execution Oversight**
- [ ] AI Chatbot: "Start recovery procedures for [System Name]"
- [ ] Real-time progress monitoring
- [ ] Executive status updates every 30 minutes
- [ ] Risk assessment for additional system impacts

Phase 3: Validation and Return to Service (60-120 minutes)

- [ ] **System Validation (NIST CP-10(6))**
- [ ] AI Chatbot: "Run validation checklist for [System Name]"
- [ ] Functional testing coordination
- [ ] Performance verification
- [ ] Security controls validation
- [ ] Integration testing with dependent systems
- [ ] **Business Sign-off**
- [ ] AI Chatbot: "Request business approval for [System Name] go-live"
- [ ] User acceptance testing results
- [ ] Business stakeholder approval
- [ ] Communication to all affected users

F.2 System-Specific Recovery Procedures

F.2.1 SAP ERP System Recovery (Mission-Critical)

AI Chatbot Guided Recovery Process:

Pre-Recovery Assessment (5 minutes)

- [ ] **Chatbot Query:** "Assess SAP ERP failure impact"
- [ ] Check HANA database status and replication
- [ ] Verify application server availability
- [ ] Review system logs and error messages
- [ ] Assess financial reporting impact ($2M+ daily transactions)

Recovery Execution (45-90 minutes)

- [ ] **Database Recovery (NIST CP-9)**
- [ ] Chatbot: "Initiate HANA database recovery procedures"
- [ ] Stop all SAP application services
- [ ] Execute HANA system replication failover
- [ ] Validate database consistency and performance
- [ ] Verify HANA tenant databases
- [ ] **Application Layer Recovery (NIST CP-10)**
- [ ] Chatbot: "Start SAP application server recovery"
- [ ] Restore application server configurations
- [ ] Start central services and message server
- [ ] Initialize work processes and RFC connections
- [ ] Verify system landscape connectivity

Business Validation (30 minutes)

- [ ] **Functional Testing**
- [ ] Chatbot: "Execute SAP critical transaction tests"
- [ ] Test Financial (FI) module transactions
- [ ] Verify Materials Management (MM) processes
- [ ] Check Sales & Distribution (SD) functions

- [ ] Validate integration with POS systems

Expected Recovery Timeline: 2 hours (within RTO) **Success Criteria:** All critical business processes operational

F.2.2 Oracle POS System Recovery (Revenue-Critical)

Emergency Response (1-Hour RTO)

Immediate Actions (5 minutes)

- [ ] **Chatbot Alert:** "POS system failure detected - 450 stores affected"
- [ ] Activate emergency cash-only procedures if needed
- [ ] Notify all regional store managers
- [ ] Assess payment gateway connectivity
- [ ] Determine if customer loyalty system affected

Recovery Execution (45 minutes)

- [ ] **Oracle RAC Failover (NIST CP-7)**
- [ ] Chatbot: "Execute Oracle RAC failover to Melbourne site"
- [ ] Initiate Data Guard switchover procedures
- [ ] Validate database cluster connectivity
- [ ] Verify transaction log synchronization
- [ ] Test POS terminal connectivity across all stores
- [ ] **System Validation (NIST CP-10(6))**
- [ ] Chatbot: "Run POS system validation checklist"
- [ ] Test transaction processing capability
- [ ] Verify payment gateway integration
- [ ] Check customer loyalty program connectivity
- [ ] Validate receipt printing and cash drawer functions

Return to Service (10 minutes)

- [ ] **Store Operations Coordination**
- [ ] Chatbot: "Notify all stores - POS systems operational"
- [ ] Coordinate with regional store managers
- [ ] Resume normal payment processing
- [ ] Monitor transaction volumes and error rates
- [ ] Provide executive status update

F.2.3 Customer Loyalty Platform Recovery

Data Protection Priority Recovery (NIST SC-13)

Assessment Phase (10 minutes)

- [ ] **Privacy Impact Assessment**
- [ ] Chatbot: "Assess customer data exposure risk"
- [ ] Determine if personal information compromised
- [ ] Check encryption key integrity
- [ ] Verify access control enforcement
- [ ] Assess notification requirements under Privacy Act

Recovery Phase (90 minutes)

- [ ] **SQL Server Always On Recovery**
- [ ] Chatbot: "Initiate SQL Server failover procedures"
- [ ] Execute Always On Availability Group failover
- [ ] Validate data consistency across replicas
- [ ] Verify customer data integrity and completeness
- [ ] Test mobile app and POS integration

Compliance Validation (30 minutes)

- [ ] **Privacy and Security Verification**
- [ ] Chatbot: "Run privacy compliance checklist"
- [ ] Verify encryption of customer personal data
- [ ] Validate access controls and audit logging
- [ ] Check integration with marketing platforms
- [ ] Confirm notification procedures if data breach

F.3 Infrastructure Recovery Procedures

F.3.1 Virtualization Infrastructure Recovery (NIST CP-6)

VMware vSphere Environment Recovery

- [ ] **Assessment and Planning**
- [ ] Chatbot: "Assess VMware infrastructure failure scope"
- [ ] Identify failed hosts and affected VMs
- [ ] Check vCenter Server and ESXi host status
- [ ] Verify shared storage availability
- [ ] Review Veeam backup repositories
- [ ] **Recovery Execution**
- [ ] Chatbot: "Execute VM instant recovery procedures"
- [ ] Power off affected VMs if still accessible
- [ ] Initiate Veeam Instant VM Recovery
- [ ] Verify VM boot and OS functionality
- [ ] Test application services and network connectivity
- [ ] **Migration and Cleanup**
- [ ] Storage vMotion from backup to production storage
- [ ] Remove temporary instant recovery objects

- [ ] Update VM configuration and tools
- [ ] Resume normal backup schedules

Expected Recovery Time: 15-30 minutes per VM

F.3.2 Network Infrastructure Recovery (NIST SC-7)

Critical Network Services Recovery

- [ ] **Immediate Response**
- [ ] Chatbot: "Activate network redundancy protocols"
- [ ] Verify failover to secondary network paths
- [ ] Check critical service connectivity (DNS, DHCP, AD)
- [ ] Coordinate with Telstra for WAN connectivity
- [ ] **Recovery Actions**
- [ ] Deploy replacement hardware if required
- [ ] Restore network configuration from backups
- [ ] Test network segmentation and VLAN functionality
- [ ] Validate security policies and firewall rules
- [ ] **Service Restoration**
- [ ] Gradually restore network traffic
- [ ] Monitor performance, latency, and packet loss
- [ ] Update network documentation and diagrams
- [ ] Schedule post-incident network assessment

F.4 DR Manager Dashboard Metrics (Sarah Chen's KPIs)

F.4.1 Real-Time Recovery Metrics

Metric	Target	Current Status	Trend
Recovery Time (RTO)	<2 hours Tier 1	In Progress: 45 min	✅ On Track
Data Loss (RPO)	<15 min Tier 1	Last Backup: 8 min	✅ Within Target
Team Response Time	<15 min	Responded: 12 min	✅ Met Target
Business Impact	Minimize	2 stores affected	⚠️ Monitor

F.4.2 AI Chatbot Performance Metrics

Metric	Target	Current Performance
Query Response Time	<3 seconds	1.8 seconds average
Procedure Accuracy	99%	99.2% validation rate
User Satisfaction	>90%	94% positive feedback
Automation Success	95%	97% successful workflows

F.5 Post-Recovery Validation Checklist

F.5.1 Technical Validation (NIST CP-10(6))

- [ ] **System Performance**
- [ ] Database response times within baseline
- [ ] Application performance metrics normal
- [ ] Network latency and throughput optimal
- [ ] Storage I/O performance validated
- [ ] **Security Validation (NIST SC Family)**
- [ ] Access controls functioning correctly
- [ ] Encryption services operational
- [ ] Audit logging capturing all activities
- [ ] Security monitoring alerts functional

- [ ] **Integration Testing**
- [ ] All system interfaces operational
- [ ] Data synchronization working
- [ ] Third-party integrations functioning
- [ ] Real-time replication validated

F.5.2 Business Validation

- [ ] **Operational Testing**
- [ ] Critical business processes working
- [ ] Store operations fully functional
- [ ] Customer services available
- [ ] Financial reporting operational
- [ ] **Stakeholder Sign-off**
- [ ] Business unit manager approval
- [ ] Regional store manager confirmation
- [ ] IT operations team validation
- [ ] DR Manager final approval

DOCUMENT CONTROL AND REVISION HISTORY

Document Information

- **Total Pages:** 52
- **Word Count:** ~18,000 words
- **NIST Framework:** SP 800-53 Rev 5, CSF 2.0, SP 800-34 Rev 1 aligned
- **Last Updated:** January 2025
- **Next Review Date:** July 2025

- **Classification:** Internal Use Only

AI Chatbot Integration Notes

- **Designed for DR Manager Persona:** Sarah Chen, CBCP certified
- **ServiceNow Integration:** Automated ticket creation and updates
- **Microsoft Teams Bot:** Voice and text command interface
- **Mobile App Support:** Field operations and store coordination
- **Executive Reporting:** Automated status updates and dashboards

Distribution List (NIST PM-1 Compliant)

Role	Name	Department	Access Level
CEO	Sarah Johnson	Executive	Read Only
CIO	Robert Taylor	IT	Full Access
DR Manager	**Sarah Chen**	**DR Operations**	**Full Edit Access**
Security Manager	Amanda Foster	Information Security	Read/Comment
Compliance Manager	Helen Mitchell	Risk & Compliance	Read/Comment
All DR Specialists	DR Team	IT Operations	Read/Execute

Revision History

Version	Date	Author	Changes
1.0	January 2025	IT Policy Team	Initial version with PCI requirements
2.0	January 2025	DR Policy Team	NIST framework alignment, PCI removal, AI chatbot integration

Final Approval Required From:

- [ ] Chief Information Officer (Robert Taylor)
- [ ] Chief Executive Officer (Sarah Johnson)
- [ ] **Disaster Recovery Manager (Sarah Chen)** - Primary Owner
- [ ] Security Manager (Amanda Foster)
- [ ] Compliance Manager (Helen Mitchell)
