Controls and Audit / Controles y Auditoría

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

November 11, 2025

1 Controls and Audit / Controles y Auditoría

1.1 EN: Audit and Control Framework

1.1.1 Evidence Pack Components

The Finanzas SD system maintains comprehensive audit trails and evidence packs for compliance and forensic analysis.

1. Application Logs **Location**: Amazon CloudWatch Logs **Retention**: 10 years **Contents**: - API request/response logs - Lambda function execution logs - Authentication events - Authorization decisions - Error logs and stack traces - Performance metrics

Log Format:

[] { ”timestamp”: ”2024-11-10T06:45:00Z”, ”requestId”: ”abc-123-def”, ”userId”: ”user@example.com”, ”action”: ”CREATE_INVOICE”, ”entityId”: ”inv-2024-001”, ”ipAddress”: ”192.168.1.100”, ”userAgent”: ”Mozilla/5.0...”, ”status”: ”SUCCESS”, ”duration”: 245 }

2. Audit Trail **Location**: DynamoDB `audit_logs` table **Retention**: 10 years **Contents**: - User actions (create, update, delete, approve, reject) - Data changes (before/after snapshots) - Access attempts (successful and failed) - Policy evaluations - Document generation events - SharePoint operations

Audit Record Format:

[] { ”logId”: ”log-2024-11-10-12345”, ”timestamp”: ”2024-11-10T06:45:00Z”, ”userId”: ”user@example.com”, ”action”: ”APPROVE_INVOICE”, ”entityId”: ”inv-2024-001”, ”changes”: { ”status”: {”from”: ”pending”, ”to”: ”approved”}, ”approvedBy”: {”from”: **null**, ”to”: ”fin@example.com”}, ”approvalDate”: {”from”: **null**, ”to”: ”2024-11-10T06:45:00Z”} }, ”ipAddress”: ”192.168.1.100”, ”userAgent”: ”Mozilla/5.0...” }

3. CloudWatch Alarms **Purpose**: Real-time monitoring and alerting **Metrics Monitored**: - API error rate > 5% - Lambda execution errors - DynamoDB throttling events - Authentication failures > 10/hour - Unauthorized access attempts - Budget threshold violations

Alarm Actions: - SNS notifications to operations team - Automatic incident ticket creation - PagerDuty escalation (for critical alarms)

4. AWS CloudTrail **Purpose**: AWS service audit trail **Retention**: 10 years **Contents**: - IAM role assumptions - S3 bucket operations - DynamoDB table operations - Lambda function invocations - Cognito authentication events - AVP policy evaluations

5. Canary Tests **Purpose**: Continuous availability monitoring **Frequency**: Every 5 minutes **Test Cases**: - User authentication flow - Budget query API - PDF generation function - SharePoint connectivity - Database read/write operations

Canary Metrics: - Success rate - Response time (p50, p95, p99) - Error rate - Availability percentage

1.1.2 Control Framework

Preventive Controls

1. **Authentication**
    - Multi-factor authentication (MFA) required for all users
    - Password complexity requirements
    - Account lockout after 5 failed attempts
    - Session timeout after 30 minutes of inactivity
2. **Authorization**
    - Role-based access control (RBAC) via AVP
    - Attribute-based access control (ABAC) for fine-grained permissions
    - Segregation of duties enforcement
    - Least privilege principle
3. **Input Validation**
    - Server-side validation for all inputs
    - SQL injection prevention
    - XSS attack prevention
    - File upload restrictions (type, size)
4. **Budget Controls**
    - Budget adjustments require approval
    - Alert when budget utilization > 80%
    - Automatic rejection when budget exceeded

Detective Controls

1. **Monitoring**
    - Real-time CloudWatch dashboards

- Anomaly detection for unusual patterns
- Failed login attempt tracking
- Budget variance monitoring

2. **Audit Logging**
    - All user actions logged
    - All data changes logged with before/after snapshots
    - All access attempts logged
    - Log integrity verification
3. **Alerts**
    - Budget threshold alerts
    - Security event alerts
    - Performance degradation alerts
    - Failed operation alerts
4. **Reporting**
    - Daily operations summary
    - Weekly security report
    - Monthly compliance report
    - Quarterly audit report

Corrective Controls

1. **Incident Response**
    - Documented incident response procedures
    - Escalation paths defined
    - Root cause analysis required
    - Remediation tracking
2. **Backup and Recovery**
    - DynamoDB point-in-time recovery enabled
    - S3 versioning enabled
    - Cross-region replication for critical data
    - Recovery time objective (RTO): 4 hours
    - Recovery point objective (RPO): 1 hour
3. **Patch Management**
    - Monthly security patching
    - Critical patches within 48 hours

- Testing in non-production first
- Rollback procedures documented

1.1.3 Compliance Requirements

SOX Compliance

- Segregation of duties enforced
- Financial data integrity controls
- Audit trail completeness
- Evidence retention (7 years minimum)

GDPR Compliance (if applicable)

- Right to access data
- Right to delete data
- Data encryption at rest and in transit
- Privacy impact assessments

Internal Audit Requirements

- Quarterly access reviews
- Annual security assessments
- Penetration testing (annual)
- Disaster recovery testing (biannual)

1.1.4 Key Performance Indicators (KPIs)

1. **Security KPIs**
   - Authentication success rate: > 99.9%
   - Unauthorized access attempts: 0
   - Security incidents: 0
   - MFA adoption rate: 100%
2. **Operational KPIs**
   - System availability: > 99.5%
   - API response time (p95): < 500ms
   - PDF generation time: < 30s
   - Error rate: < 0.1%
3. **Audit KPIs**
   - Audit log completeness: 100%

- Finding remediation time: < 30 days
- Compliance score: > 95%
- Evidence pack completeness: 100%

1.2 ES: Marco de Auditoría y Control

1.2.1 Componentes del Paquete de Evidencia

El sistema Finanzas SD mantiene registros de auditoría exhaustivos y paquetes de evidencia para cumplimiento y análisis forense.

[Traducción de todas las secciones de controles y auditoría]

1.2.2 Marco de Control

Controles Preventivos [Traducción de controles preventivos]

Controles Detectivos [Traducción de controles detectivos]

Controles Correctivos [Traducción de controles correctivos]

1.2.3 Requisitos de Cumplimiento

Cumplimiento SOX [Traducción de requisitos]

Indicadores Clave de Rendimiento (KPI) [Traducción de KPIs]