SecureVault Compliance Reporting Guide

Document ID: PRD-SV-025 **Last Updated:** 2024-02-15 **Owner:** SecureVault Product Team **Classification:** Public

---

Overview

SecureVault provides comprehensive compliance reporting to help organizations meet regulatory requirements. This guide covers audit logs, compliance reports, and evidence collection for SOC 2, ISO 27001, PCI-DSS, HIPAA, and GDPR.

Compliance Dashboard

Accessing the Dashboard

Navigate to **SecureVault → Compliance → Dashboard**

Dashboard Components

Widget	Description
Compliance Score	Overall compliance health (0-100)
Policy Violations	Active violations by severity
Audit Activity	Recent audit events
Certificate Status	Expiring certificates
Access Reviews	Pending access reviews

Built-in Compliance Reports

SOC 2 Reports

Access Control Report

```
# Generate SOC 2 access control report
securevault compliance report \
  --type soc2-access-control \
  --start-date 2024-01-01 \
  --end-date 2024-03-31 \
  --output soc2-access-q1.pdf
```

Report includes: - User access provisioning/deprovisioning - Privileged access usage - Access review completion - Authentication failures - MFA enrollment status

Change Management Report

```
securevault compliance report \
  --type soc2-change-management \
  --period Q1-2024
```

Report includes: - Secret modifications - Policy changes - Configuration updates - Approval workflows - Emergency changes

ISO 27001 Reports

Asset Inventory Report

```
securevault compliance report \
  --type iso27001-assets \
  --format xlsx
```

Report includes: - All secrets inventory - Classification levels - Data owners - Retention policies - Encryption status

Risk Assessment Report

```
securevault compliance report \
  --type iso27001-risk \
  --include-mitigations
```

PCI-DSS Compliance

Requirement Mapping

PCI-DSS Requirement	SecureVault Feature
3.4 - Render PAN unreadable	AES-256 encryption
3.5 - Protect encryption keys	HSM integration
3.6 - Key management	Automatic rotation
7.1 - Limit access	RBAC policies
7.2 - Access control system	Policy enforcement
8.2 - Authentication	MFA required
10.1 - Audit trails	Comprehensive logging

Cardholder Data Report

```
securevault compliance report \
  --type pci-dss \
  --scope cardholder-data \
  --assessor-mode
```

Report includes: - All PAN-related secrets - Access logs for cardholder data - Encryption verification - Key rotation history - Segmentation evidence

Key Management Evidence

```yaml
# pci-key-management.yaml
compliance:
  pci_dss:
    key_management:
      generation:
        method: HSM
        algorithm: AES-256
        entropy_source: hardware_rng
      storage:
        location: HSM
        access: dual_control
      rotation:
        frequency: annual
        automated: true
      destruction:
        method: cryptographic_erasure
        verification: required
```

HIPAA Compliance

PHI Access Report

```
securevault compliance report \
  --type hipaa-phi-access \
  --patient-data-only \
  --period last-90-days
```

Report includes: - All PHI-related secret access - User justification (if required) - Emergency access (break-glass) - Minimum necessary verification

Security Rule Evidence

```
# hipaa-controls.yaml
compliance:
  hipaa:
    administrative:
      security_officer: assigned
      risk_analysis: completed
      workforce_training: 97%
    physical:
      facility_access: controlled
      workstation_security: enforced
    technical:
      access_control: rbac
      audit_controls: enabled
      integrity_controls: enabled
      transmission_security: tls_1_3
```

Breach Notification Readiness

```
# Generate breach assessment data
securevault compliance breach-assessment \
  --secret-path "secret/phi/*" \
  --timeframe "2024-07-01 to 2024-07-15"
```

GDPR Compliance

Data Subject Access Request (DSAR)

```
# Find all secrets related to a data subject
securevault compliance dsar \
  --subject-identifier "user@example.com" \
  --output dsar-response.json
```

Response includes: - Secrets containing subject data - Access history - Processing purposes - Retention periods - Third-party sharing

Right to Erasure

```
# Identify secrets for deletion
securevault compliance erasure-request \
  --subject-identifier "user@example.com" \
  --dry-run

# Execute erasure with audit trail
securevault compliance erasure-request \
  --subject-identifier "user@example.com" \
  --execute \
  --reason "GDPR Article 17 request"
```

Data Processing Inventory

```
securevault compliance report \
  --type gdpr-processing-inventory \
  --include-legal-basis
```

Audit Log Management

Log Configuration

```
# audit-config.yaml
audit:
  enabled: true
  log_level: detailed

  events:
```

```
    - secret_read
    - secret_write
    - secret_delete
    - policy_change
    - auth_success
    - auth_failure
    - config_change

  destinations:
    - type: internal
      retention: 2_years
    - type: siem
      endpoint: https://siem.novatech.internal
      format: CEF
    - type: s3
      bucket: novatech-audit-logs
      encryption: AES-256
```

Querying Audit Logs

```
# Search audit logs
securevault audit search \
  --action "secret_read" \
  --path "secret/production/*" \
  --start "2024-07-01" \
  --end "2024-07-31"

# Export for external analysis
securevault audit export \
  --format json \
  --start "2024-01-01" \
  --end "2024-06-30" \
  --output audit-h1-2024.json
```

Log Integrity Verification

```
# Verify log chain integrity
securevault audit verify-integrity \
  --start "2024-01-01" \
  --end "2024-07-31"

# Output
Log Integrity Check
===================
```

```
Total records: 1,234,567
Chain valid:
Hash verification:
Timestamp ordering:
No gaps detected:
```

Evidence Collection

Automated Evidence Package

```
# Generate comprehensive evidence package
securevault compliance evidence-package \
  --frameworks soc2,iso27001,pci-dss \
  --period 2024-Q2 \
  --output evidence-q2-2024/
```

Package contents:

```
evidence-q2-2024/
   soc2/
       access-control-evidence.pdf
       change-management-evidence.pdf
       monitoring-evidence.pdf
   iso27001/
       asset-inventory.xlsx
       risk-assessment.pdf
       control-matrix.xlsx
   pci-dss/
       requirement-3-evidence.pdf
       requirement-7-evidence.pdf
       requirement-10-evidence.pdf
   manifest.json
```

Custom Evidence Collection

```
# evidence-collection.yaml
evidence:
  name: Q2-2024-Audit
  period:
    start: 2024-04-01
    end: 2024-06-30
```

```yaml
  collections:
    - name: access-reviews
      type: report
      source: access_review_completions

    - name: privileged-access
      type: audit_log
      filter:
        policy: admin-policy

    - name: encryption-status
      type: configuration
      paths:
        - secret/data/*

    - name: rotation-compliance
      type: metrics
      metric: secret_rotation_compliance
```

Compliance Policies

Policy Configuration

```yaml
# compliance-policies.yaml
policies:
  - name: secret-classification
    description: All secrets must be classified
    rule:
      type: metadata_required
      fields:
        - classification
        - owner
        - retention_period
    enforcement: block

  - name: rotation-requirement
    description: Secrets must rotate within policy
    rule:
      type: rotation_compliance
      max_age_days: 90
    enforcement: alert
```

```yaml
  - name: access-justification
    description: Access requires justification
    rule:
      type: access_justification
      paths:
        - secret/pci/*
        - secret/phi/*
    enforcement: block
```

Policy Violation Alerts

```yaml
# Alert configuration
alerts:
  compliance_violations:
    channels:
      - type: email
        recipients:
          - compliance@novatech.com
          - security@novatech.com
      - type: slack
        channel: "#compliance-alerts"
      - type: pagerduty
        severity_mapping:
          critical: P1
          high: P2
          medium: P3
```

Scheduled Reports

Report Automation

```yaml
# scheduled-reports.yaml
scheduled_reports:
  - name: weekly-compliance-summary
    schedule: "0 8 * * MON"
    type: compliance-summary
    recipients:
      - security-team@novatech.com
    format: pdf

  - name: monthly-access-review
    schedule: "0 9 1 * *"
```

```
    type: access-review
    recipients:
      - managers@novatech.com
    format: xlsx

  - name: quarterly-soc2-evidence
    schedule: "0 9 1 1,4,7,10 *"
    type: soc2-full
    recipients:
      - compliance@novatech.com
    output:
      type: s3
      bucket: compliance-reports
```

Integration with GRC Tools

ServiceNow GRC

```
integration:
  servicenow:
    instance: novatech.service-now.com
    sync:
      - controls_evidence
      - policy_violations
      - risk_assessments
    schedule: daily
```

OneTrust

```
integration:
  onetrust:
    sync:
      - data_inventory
      - processing_activities
      - dsar_responses
```

Best Practices

Report Management

1. **Automate evidence collection** for audit efficiency
2. **Maintain report archives** for trend analysis
3. **Review violations weekly** with remediation plans
4. **Test controls quarterly** before audits

Audit Preparation

1. **Pre-audit health check** 30 days before
2. **Evidence package review** with auditors
3. **Control owner briefings** on evidence
4. **Gap remediation** with documented plans

Troubleshooting

Common Issues

Issue	Solution
Report generation slow	Reduce date range, use filters
Missing audit events	Check audit configuration
Evidence gaps	Review collection schedule
Export failures	Verify destination permissions

Related Documents: Audit Logging (PRD-SV-020), Access Policies (PRD-SV-015), Security Best Practices (PRD-SV-050)