SOC2 Compliance Assessment Report

Generated on May 15, 2025
Scan ID: SOC2-c4985b38
Source: github - https://github.com/prowler-cloud/prowler

Compliance Summary

Overall Compliance

54.8%
Critical

Metric	Value
Total Checks	62
Passed Checks	34
Failed Checks	28
Compliance Score	54.8%

Category Compliance

Category	Total	Passed	Failed	Score
Security	14	8	6	57.1%
Availability	12	6	6	50.0%
Processing Integrity	12	8	4	66.7%
Confidentiality	12	8	4	66.7%
Privacy	12	4	8	33.3%

Critical Violations

V-83ee37: Systems implement strong authentication mechanisms (e.g., MFA)

Category: Security - Access Controls
Impact: High: Systems without strong authentication are vulnerable to unauthorized access
Examples:
• Single-factor authentication used for critical systems
• MFA not enforced for administrative access
Recommended Actions:
• Implement MFA for all administrative access
• Enable MFA for all user accounts

V-6f470b: Regular risk assessments are performed

Category: Security - Risk Mitigation
Impact: Unknown

V-92a4d6: Systems are monitored for performance and availability

Category: Availability - Performance Monitoring
Impact: High: Unmonitored systems may experience undetected outages
Examples:
• No system monitoring tools in place
• Alerts not configured for critical services
Recommended Actions:
• Implement comprehensive monitoring solution
• Configure alerting for all critical services

V-550e45: Formal disaster recovery plan exists and is tested

Category: Availability - Disaster Recovery
Impact: High: Without a tested DR plan, recovery may be delayed or impossible
Examples:
• No formal disaster recovery plan
• DR plan exists but has never been tested
Recommended Actions:
• Develop comprehensive DR plan
• Conduct annual DR testing

V-0c48b8: Recovery time objectives (RTOs) are defined and tested

Category: Availability - Disaster Recovery
Impact: Unknown

13 more high-risk violations...

Key Recommendations

1. Improve Security Access Controls

Category: Security - Access Controls
Description: Address 3 security access controls violations
Implementation Steps:
• Implement MFA for all administrative access

• Enable MFA for all user accounts
• Implement automated user provisioning/deprovisioning
• Conduct quarterly account reviews
• Enforce minimum 12-character passwords
• Implement password complexity requirements

2. Improve Security Risk Mitigation

Category: Security - Risk Mitigation
Description: Address 1 security risk mitigation violations

3. Improve Availability Performance Monitoring

Category: Availability - Performance Monitoring
Description: Address 1 availability performance monitoring violations
Implementation Steps:
• Implement comprehensive monitoring solution
• Configure alerting for all critical services

4. Improve Availability Disaster Recovery

Category: Availability - Disaster Recovery
Description: Address 2 availability disaster recovery violations
Implementation Steps:
• Develop comprehensive DR plan
• Conduct annual DR testing

5. Improve Availability Backup Systems

Category: Availability - Backup Systems
Description: Address 1 availability backup systems violations

8 more high-priority recommendations...

SOC2 Trust Services Criteria

Security (57.1%)

Protection of system resources against unauthorized access

Principle	Checks	Score
Access Controls	1/4	25.0%
System Operations	3/4	75.0%
Change Management	2/3	66.7%
Risk Mitigation	2/3	66.7%

Availability (50.0%)

System availability for operation and use as committed or agreed

Principle	Checks	Score
Performance Monitoring	2/3	66.7%
Disaster Recovery	1/3	33.3%
Backup Systems	2/3	66.7%
Business Continuity	1/3	33.3%

Processing Integrity (66.7%)

System processing is complete, valid, accurate, timely, and authorized

Principle	Checks	Score
Data Validation	1/3	33.3%
Transaction Authorization	2/3	66.7%
Input/Output Controls	2/3	66.7%
Error Handling	3/3	100.0%

Confidentiality (66.7%)

Information designated as confidential is protected as committed or agreed

Principle	Checks	Score
Data Classification	1/3	33.3%
Encryption	2/3	66.7%
Information Lifecycle	2/3	66.7%
Confidentiality Agreements	3/3	100.0%

Privacy (33.3%)

Personal information is collected, used, retained, disclosed, and disposed of in conformity with commitments

Principle	Checks	Score
Notice and Communication	2/3	66.7%
Choice and Consent	1/3	33.3%
Collection and Use	1/3	33.3%
Access and Disclosure	0/3	0.0%