

# Panguard AI - iso27001 Compliance Report

## ISO/IEC 27001:2022

Generated: 2026-05-19

Organization: Acme Corp (Sample)

# Executive Summary

---

## Overall Compliance Score: 77%

Total Controls: 30  
Passed: 21 | Failed: 5 | Partial: 4 | N/A: 0  
Total Findings: 5  
Critical: 0 | High: 2

### Key Risks:

- Information Security for Use of Cloud Services
- Configuration Management
- Monitoring Activities

### Key Achievements:

- 21 controls fully compliant
  - No critical findings
-

# Findings

---

HIGH

FW-001

## Firewall disabled

macOS Application Firewall is disabled. System is exposed to inbound connections.

---

HIGH

NET-PORT-001

## Risky services exposed

The following services are listening on network interfaces: Redis (6379), Redis (6379), PostgreSQL (5432), PostgreSQL (5432). These should be firewalled or disabled.

---

MEDIUM

IR-NOTIFY-001

## No notification channels configured

Panguard has no notification channels (Telegram/Slack/Email) configured. Incident alerts cannot be delivered.

---

MEDIUM

MON-LOG-002

## System logging may be impaired

Could not verify macOS unified log status.

---

MEDIUM

PATCH-001

## 2 pending system updates

There are 2 pending macOS software updates. Security patches should be applied promptly.

---

# Compliance Overview

Control ID	Title	Status	Findings
A.5.1	Policies for Information Security	Pass	-
A.5.2	Information Security Roles and Respon...	Pass	-
A.5.10	Acceptable Use of Information and Oth...	Pass	-
A.5.15	Access Control	Pass	-
A.5.17	Authentication Information	Pass	-
A.5.23	Information Security for Use of Cloud...	Fail	1 finding
A.5.24	Information Security Incident Managem...	Partial	1 finding
A.5.28	Collection of Evidence	Partial	1 finding
A.5.29	Information Security During Disruption	Pass	-
A.5.30	ICT Readiness for Business Continuity	Pass	-
A.5.36	Compliance with Policies and Standards	Pass	-
A.6.1	Screening	Pass	-
A.6.3	Information Security Awareness, Educa...	Pass	-
A.7.1	Physical Security Perimeters	Pass	-
A.7.4	Physical Security Monitoring	Pass	-
A.8.1	User Endpoint Devices	Pass	-
A.8.2	Privileged Access Rights	Pass	-
A.8.3	Information Access Restriction	Pass	-
A.8.5	Secure Authentication	Pass	-
A.8.7	Protection Against Malware	Pass	-
A.8.8	Management of Technical Vulnerabilities	Partial	1 finding
A.8.9	Configuration Management	Fail	1 finding
A.8.12	Data Leakage Prevention	Pass	-
A.8.13	Information Backup	Pass	-
A.8.15	Logging	Partial	1 finding
A.8.16	Monitoring Activities	Fail	1 finding
A.8.20	Network Security	Fail	2 findings
A.8.21	Security of Network Services	Fail	2 findings
A.8.24	Use of Cryptography	Pass	-
A.8.25	Secure Development Life Cycle	Pass	-























