

# Panguard AI - tw\_cyber\_security\_act Compliance Report

Generated: 2026-05-19

Organization: Acme Corp (Sample)

# Executive Summary

---

## Overall Compliance Score: 65%

Total Controls: 10  
Passed: 5 | Failed: 2 | Partial: 3 | N/A: 0  
Total Findings: 5  
Critical: 0 | High: 2

### Key Risks:

- System and Communication Protection
- Network Security Management

### Key Achievements:

- 5 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

MON-LOG-002

## System logging may be impaired

Could not verify macOS unified log status.

---

MEDIUM

IR-NOTIFY-001

## No notification channels configured

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

---

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
TWCS-4.1	Access Control and Identity Management	Pass	-
TWCS-4.2	System and Communication Protection	Fail	2 findings
TWCS-4.3	Network Security Management	Fail	1 finding
TWCS-4.4	Encryption and Key Management	Pass	-
TWCS-4.5	Multi-Factor Authentication	Pass	-
TWCS-4.6	Security Monitoring and Log Management	Partial	1 finding
TWCS-4.7	Security Incident Response	Partial	1 finding
TWCS-4.8	Information Asset Management	Pass	-
TWCS-4.9	Vulnerability and Patch Management	Partial	1 finding
TWCS-4.10	Security Audit and Assessment	Pass	-























