



GRC (TECHNICAL) COMPLIANCE REPORT

ISO 27001 Statement of Applicability

Independent verification of control implementation against ISO/IEC 27001 Annex A.

Prepared for

GRC (Technical)

Snapshot ID

5faaf096-7dd9-4b30-82cd-88713fcb06ff

Framework

ISO27001

Endpoints Assessed

14

Generated

2026-10-14 05:02:55 UTC

Evidence Signature

b1b63da4886ab687

Produced by LEA — Continuous Compliance & Control Validation Platform

This report was generated directly from signed, tamper-evident evidence collected by **LEA** (gsr-lea.com), a continuous compliance and attack-surface validation platform engineered by **GSR-IT** (gsr-it.com). LEA evaluates system state directly against industry control frameworks — CIS Benchmarks, ISO/IEC 27001, SOC 2, and CMMC — using read-only, low-privilege checks, and cryptographically signs every result at the point of collection so findings can be independently verified rather than taken on trust.

Executive Summary



87%

of tested ISO27001 controls are passing across 14 endpoint(s) as of 2026-10-14 05:02:55 UTC.

ISO27001 controls are in a strong state across the assessed environment. Continued periodic validation is recommended to maintain this posture as systems change.

11

CONTROLS TESTED

91

PASSING

14

FAILING

14

ENDPOINTS



Why, What & How We Tested

WHY

This assessment provides independent, evidence-based assurance that ISO27001 controls are operating as intended, supporting your organization's risk management, regulatory, and customer-assurance obligations. Results are produced by LEA rather than self-reported.

WHAT

11 ISO27001 controls were evaluated across 14 in-scope endpoint(s), covering the categories mapped to this framework by LEA's rule catalog (access control, logging, network exposure, patching, and related domains).

HOW

Each control was tested with a low-privilege, read-only validation command executed on-host by the LEA agent, sampling raw system state (e.g. the /proc filesystem, configuration files) rather than relying on interviews or self-attestation. Every result was HMAC-signed at collection time and written to an append-only evidence ledger.

GRC Technical Report — Control Gap Analysis

Complete control-by-control gap analysis against ISO27001, including the full control description and current implementation status, for use in control-owner review and remediation tracking.

CONTROL ID	CONTROL NAME	DESCRIPTION	CATEGORY	SEVERITY	STATUS
ISO27001-A.10.1.1	Disk Encryption Enabled (macOS)	Ensures FileVault full-disk encryption is enabled on the system.	system_hardening	MEDIUM	Gap Identified
ISO27001-A.11.2.9	macOS Screen Lock Short Delay	Ensures macOS is configured to require a password shortly after sleep or screen saver begins (e.g., within 5 minutes).	access_control	MEDIUM	Gap Identified
ISO27001-A.13.1.1	Linux Firewall Service Running	Ensures a host-based firewall service (ufw, firewalld, or iptables-based front-end) is running on Linux systems.	network_security	MEDIUM	Gap Identified
ISO27001-A.9.2.3	No Unauthorized UID 0 Accounts	Ensures no user accounts other than 'root' have a UID of 0 (full administrative privileges).	identity_management	MEDIUM	Gap Identified
ISO27001-A.9.4.2	Account Lockout Policy Configured	Checks that accounts are locked out after a limited number of failed login attempts.	authentication	MEDIUM	Gap Identified
ISO27001-A.9.4.3	Directory Password Complexity Enforced	Ensures directory and local macOS account policies enforce password complexity, including mixed case, numeric, and symbol characters, and Active Directory complexity is enabled.	password_policy	MEDIUM	Gap Identified
ISO27001-A.12.2.1	Anti-Malware Service Running	Verifies that an anti-malware (anti-virus) protection service is active on the system (e.g., Windows Defender).	integrity	MEDIUM	Implemented
ISO27001-A.12.4.1	Audit Log Retention Configured	Ensures the audit daemon is configured not to automatically delete or overwrite old logs (e.g., using 'keep_logs').	audit	MEDIUM	Implemented
ISO27001-A.12.6.2	Blacklisted Offensive Tools Not Running	Ensures no known offensive security or cracking tools (such as nmap, sqlmap, hydra, john, hashcat, aircrack-ng, netcat, or ncat) are running as active processes on the host.	integrity	MEDIUM	Implemented
ISO27001-A.9.2.4	No Empty Passwords	Ensures no local user account has an empty password (password field blank). Required sudo rule: allow user lea to run ONLY this exact command without a password: lea ALL=(root) NOPASSWD: /bin/cat /etc/shadow	password_policy	MEDIUM	Implemented
ISO27001-A.9.2.6	Guest Account Disabled	Verifies that the built-in Guest user account is disabled to prevent interactive logon.	access_control	MEDIUM	Implemented

How the Score Was Calculated

Compliance score = (Passing Controls ÷ Total Controls Tested) × 100, evaluated per framework from the latest signed evidence snapshot (5faaf096-7dd9-4b30-82cd-88713fcb06ff, 2026-10-14 05:02:55 UTC).

A control is marked **PASS** when the on-host validation command's output matched the expected state defined for that control at collection time, and **FAIL** otherwise. Results are aggregated per control across all in-scope endpoints; the overall percentage reflects every individual host/control evidence record collected in this snapshot, not a sample. The street-light indicator on the Executive Summary applies fixed thresholds: **green** at 80% or higher, **amber** from 50–79%, and **red** below 50%.

Every evidence record in this report is cryptographically signed (HMAC-SHA256) at the moment of collection and stored in an append-only ledger (signing key fingerprint: b1b63da4886ab687), so results cannot be altered after the fact. This report was generated by the LEA platform (gsr-lea.com), built by GSR-IT (gsr-it.com). For questions about this assessment or to extend LEA's coverage to additional frameworks and endpoints, contact your GSR-IT representative.