



IT MANAGER COMPLIANCE REPORT

ISO 27001 Statement of Applicability

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

Prepared for

IT Manager

Snapshot ID

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

Framework

ISO27001

Endpoints Assessed

14

Generated

2026-10-14 05:02:54 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 05:02:54 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.

IT Manager Report — Control Detail

Full per-endpoint results for every ISO27001 control tested in snapshot 5faaf096-7dd9-4b30-82cd-88713fcb06ff. Use this table to prioritize remediation work and assign ownership across your endpoint fleet.

Failing Controls by Endpoint

CONTROL ID	RULE	CATEGORY	SEVERITY	HOST	OBSERVED VALUE	TIMESTAMP
ISO27001-A.9.2.3	No Unauthorized UID 0 Accounts	identity_management	MEDIUM	analytics-worker-04		2026-10-14T05:02:44
ISO27001-A.9.4.2	Account Lockout Policy Configured	authentication	MEDIUM	analytics-worker-04		2026-10-14T05:02:44
ISO27001-A.9.4.3	Directory Password Complexity Enforced	password_policy	MEDIUM	analytics-worker-04	# # /etc/login.defs - Configuration control definitions for the shadow package.	2026-10-14T05:02:44
ISO27001-A.9.4.3	Directory Password Complexity Enforced	password_policy	MEDIUM	analytics-worker-04	# # /etc/login.defs - Configuration control definitions for the shadow package.	2026-10-14T05:02:44
ISO27001-A.10.1.1	Disk Encryption Enabled (macOS)	system_hardening	MEDIUM	design-mbp-05	FileVault is Off.	2026-10-14T05:02:44
ISO27001-A.11.2.9	macOS Screen Lock Short Delay	access_control	MEDIUM	design-mbp-05	600	2026-10-14T05:02:44
ISO27001-A.13.1.1	Linux Firewall Service Running	network_security	MEDIUM	design-mbp-05	Firewall is disabled. (State = 0)	2026-10-14T05:02:44
ISO27001-A.9.2.3	No Unauthorized UID 0 Accounts	identity_management	MEDIUM	design-mbp-05	# \$OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp \$ # This is the	2026-10-14T05:02:44
ISO27001-A.9.4.2	Account Lockout Policy Configured	authentication	MEDIUM	design-mbp-05	# \$OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp \$ # This is the	2026-10-14T05:02:44
ISO27001-A.9.2.3	No Unauthorized UID 0 Accounts	identity_management	MEDIUM	web-frontend-01	PermitRootLogin yes PasswordAuthentication no ClientAliveInterval 300 ClientAlive	2026-10-14T05:02:44
ISO27001-A.10.1.1	Disk Encryption Enabled (macOS)	system_hardening	MEDIUM	win-files-02	BitLocker Drive Encryption: Configuration Tool version 10.0.20348 Copyright (C)	2026-10-14T05:02:44
ISO27001-A.13.1.1	Linux Firewall Service Running	network_security	MEDIUM	win-files-02	Domain Profile Settings: -----	2026-10-14T05:02:44
ISO27001-A.13.1.1	Linux Firewall Service Running	network_security	MEDIUM	win-files-02		2026-10-14T05:02:44
ISO27001-A.9.2.3	No Unauthorized UID 0 Accounts	identity_management	MEDIUM	win-files-02	User name Administrator Full Name Comme	2026-10-14T05:02:44

All Controls — Summary by Control ID

CONTROL ID	RULE	CATEGORY	SEVERITY	PASSING HOSTS	FAILING HOSTS	STATUS
ISO27001-A.10.1.1	Disk Encryption Enabled (macOS)	system_hardening	MEDIUM	3	2	FAIL
ISO27001-A.11.2.9	macOS Screen Lock Short Delay	access_control	MEDIUM	3	1	FAIL
ISO27001-A.13.1.1	Linux Firewall Service Running	network_security	MEDIUM	5	3	FAIL
ISO27001-A.9.2.3	No Unauthorized UID 0 Accounts	identity_management	MEDIUM	20	4	FAIL
ISO27001-A.9.4.2	Account Lockout Policy Configured	authentication	MEDIUM	12	2	FAIL
ISO27001-A.9.4.3	Directory Password Complexity Enforced	password_policy	MEDIUM	26	2	FAIL

ISO27001-A.12.2.1	Anti-Malware Service Running	integrity	MEDIUM	2	0	PASS
ISO27001-A.12.4.1	Audit Log Retention Configured	audit	MEDIUM	6	0	PASS
ISO27001-A.12.6.2	Blacklisted Offensive Tools Not Running	integrity	MEDIUM	2	0	PASS
ISO27001-A.9.2.4	No Empty Passwords	password_policy	MEDIUM	10	0	PASS
ISO27001-A.9.2.6	Guest Account Disabled	access_control	MEDIUM	2	0	PASS

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 05:02:54 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.