ISO/IEC 27001:2022 Annex A — evidence pack

Endpoint posture evidence for Acme (sample data) (framework version 2022)

Prepared by MigAAP — sample · data as of 23 Oct 2026 03:13 UTC · generated 23 Oct 2026 03:13 UTC

Summary

Requirements mapped	13
Met by current posture	0
Partly met	13
Gap (control not configured anywhere)	0
Unknown (not readable)	0
Overall endpoint posture score	28.7%

Framework mapping not yet verified: Control numbers follow the 2022 Annex A structure (themes 5-8); labels are our own short paraphrases. Verify against a licensed copy before customer-facing use.

Licence note: Annex A control numbers and short descriptive labels only; the standard is copyrighted by ISO and must be purchased for its text.

Requirements

Req.	Title	Relation	Controls (score)	Status
A.5.17	Authentication information	supports	Minimum password length (80%); Password complexity (0%); Password history (40%); Password expiry (40%)	partial
A.6.7	Remote working	partially supports	VPN profiles (0%); Device ownership rules (0%); Disk encryption (60%)	partial
A.7.10	Storage media	supports	USB and removable media (100%); Disk encryption (60%)	partial
A.8.1	User endpoint devices	supports	Disk encryption (60%); Screen lock and timeout (80%); Remote lock and wipe capability (0%); Minimum OS version (20%); Device ownership rules (0%); Jailbreak / root detection (50%); Enrollment restrictions (0%)	partial
A.8.2	Privileged access rights	supports	Local administrator rights (66.7%)	partial
A.8.5	Secure authentication	partially supports	Screen lock and timeout (80%); Minimum password length (80%); Certificate profiles (0%)	partial
A.8.7	Protection against malware	supports	Antivirus / anti-malware status (50%); Application blocklist (40%)	partial
A.8.8	Management of technical vulnerabilities	supports	OS patch age (40%); Update policy (0%); Minimum OS version (20%)	partial
A.8.9	Configuration management	partially supports	Host firewall (100%); Browser restrictions (0%); Local administrator rights (66.7%); Compliance grace period (0%)	partial
A.8.12	Data leakage prevention	partially supports	USB and removable media (100%); Camera and screen capture (20%); Device ownership rules (0%)	partial
A.8.19	Installation of software on operational systems	supports	Application allowlist (0%); Application blocklist (40%); Local administrator rights (66.7%)	partial

Req.	Title	Relation	Controls (score)	Status
A.8.20	Networks security	partially supports	Host firewall (100%); Wi-Fi profiles (20%); VPN profiles (0%)	partial
A.8.24	Use of cryptography	partially supports	Disk encryption (60%); Certificate profiles (0%)	partial

Data freshness

Tool	Type	Status	Last successful sync
DemoMDM	demo	healthy	2026-10-23T03:13:08+00:00

How to read this pack

Compliant/non-compliant counts come from device state the tools report (for example encryption or anti-malware health) or from OS versions checked against the configured minimum. 'Configured' means a managing tool has a readable policy for the control on that platform; policy assignment to each device is not read yet, so it is not proof that every device received it. 'Unknown' (tool policies not readable) is excluded from scores and never assumed.

Status: met = every mapped control scores 100%; partial = some devices or platforms lack the control; gap = no device has the control configured or compliant; unknown = no readable data. 'Partially supports' means the framework requirement also needs organisational evidence that tools cannot show.

This pack is technical evidence of endpoint posture. It is not a certification or an auditor's opinion.