PUBLIC EXAMPLE — SANITISED

EXECUTIVE SUMMARY

Global Corp

NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022

Compliance assessment of the Cisco Meraki cloud-managed network estate

Assessment date	26 July 2026
Assessed by	Objektiv AI — Claude Opus 5 (Anthropic)
Method	Read-only inspection of the Cisco Meraki Dashboard. No configuration was created, modified or saved.
Scope	10 networks across 5 countries · 110 devices (7 offline) · 969 clients · 19.55 TB weekly traffic
Frameworks	NIST CSF 2.0 (NIST CSWP 29, February 2024) · ISO/IEC 27001:2022 Annex A
Findings	3 critical · 5 high · 5 medium · 2 low
Classification	Public. Organisation renamed; all identifiers removed.

This report is machine-generated from open inspection of the organisation's own cloud management platform. Every finding cites the dashboard page it was read from, so any assessor can re-derive it. Figures are accurate as at the assessment date and will drift as the estate changes.

The short version

Global Corp runs a well-built, well-maintained network. Hardware is current, firmware is up to date across all ten sites, the platform records an unusually complete audit trail, and several deliberate hardening decisions have been made correctly. The estate is not neglected.

The problem is that the security features the organisation already owns are switched off, and administrative access to the whole estate rests on passwords alone.

Two findings would, on their own, be enough for an auditor to raise a major non-conformity: **multi-factor authentication is not enforced and six of fourteen administrators do not use it**, and **the malware protection and intrusion detection on the security appliances are disabled**. Both are configuration changes. Neither requires new spend.

What this means in business terms

- A single stolen administrator password gives an attacker configuration control of the network in ten countries — firewall rules, VPN tunnels, traffic mirroring. There is no second factor standing in the way for six accounts, no lockout to slow guessing, and no source-address restriction.
- If that happened, nothing would raise an alarm. Every alert in the sample network is switched off, including "configuration settings are changed". Detection currently depends on somebody choosing to read a log.
- More than half of all administrative accounts belong to five external suppliers, one of them through a shared mailbox used from two countries. Actions taken through it cannot be attributed to a person.
- Cyber insurance renewals and customer security questionnaires now routinely ask, in writing, whether MFA is enforced on network infrastructure administration. Today the honest answer is no.

What is already compliant

These are real strengths, not consolation. They are also the reason the remediation estimate is measured in days rather than months — the foundations are sound.

- A complete and attributable configuration audit trail exists. 2,495 configuration changes are retained back to 6 August 2025, each with administrator, timestamp, network, setting, old value and new value.
- Authentication events are logged in detail, including second-factor outcomes. 1,406 login attempts are retained with source IP address, geolocation, event type and outcome, and second-factor failures are recorded distinctly from password failures.
- EU data residency. Organisation data is hosted in Europe, as stated by the platform.
- Legacy SNMP is fully disabled. Both SNMP v2c and SNMP v3 are disabled at organisation level.
- Cloud CLI is restricted to read-only. The IOS-XE Cloud CLI is set to "Only read-only access" rather than configuration access, so the terminal cannot be used to change device configuration.
- Privacy-sensitive features are disabled by default on new networks. "Create new networks with privacy-sensitive features disabled by default" is enabled, so a new site does not silently begin collecting analytics data.

A further 3 confirmed strengths are listed in section 4 of the full report.

What needs to be fixed

Ordered by what an attacker would use first, not by effort.

ID	Finding	Severity	Effort
F-01	Multi-factor authentication is not enforced, and six of fourteen administrators do not use it	**Critical**	15 minutes of configuration
F-02	A personal consumer email address holds full organisation-wide administrative access and has been dormant for over two years	**Critical**	2 minutes
F-03	Malware protection and intrusion detection are switched off on the security appliances	**Critical**	1 hour per network to enable
F-04	Three site-to-site VPN tunnels use cryptography that is no longer permitted, including IKEv1, SHA-1, MD5 and 1024-bit Diffie-Hellman, with Perfect Forward Secrecy disabled	**High**	2–4 hours per tunnel including far-end coordination and a maintenance window
F-05	No single sign-on: SAML is disabled, so administrative identities are local to the dashboard and cannot be centrally revoked	**High**	1–2 days including testing and the break-glass procedure
F-06	Dormant administrator accounts are not removed; access rights are not reviewed	**High**	30 minutes now
F-07	No alerting is enabled: configuration changes, VPN failures, rogue access points and appliance outages generate no notification	**High**	30 minutes per network
F-08	Five external parties hold administrative access, one via a shared generic account used from two countries	**High**	1 day of review plus supplier correspondence
F-09	Repeated two-factor authentication failures on a shared supplier account are not investigated	**Medium**	2 hours of investigation
F-10	No account lockout, no session idle timeout, no password length or complexity requirement, and no source-IP restriction on the dashboard or its API	**Medium**	30 minutes for the account controls
F-11	Least privilege is not applied: ten of fourteen administrators hold organisation-wide full access and no limited or custom roles are in use	**Medium**	1 day of analysis and reassignme

ID	Finding	Severity	Effort
			nt
F-12	Cisco support is permitted standing full access to the organisation	**Medium**	1 hour to document, or 2 minutes to change
F-13	Logs are generated but never leave the platform: no syslog or SIEM export, and retention is bounded by the vendor	**Medium**	1–2 days depending on whether a collector already exists
F-14	Firmware is current but patching is reactive: no maintenance window is scheduled and one platform is a release behind	**Low**	2 hours to define and schedule
F-15	Ad-hoc configuration changes without evidence of change control, including a protective switch feature being disabled	**Low**	4 hours of review

Do these four things first

Together these close both critical findings and the highest-value part of two more. Total configuration effort is under a working day; the notice period, not the work, sets the timeline.

1. Enforce multi-factor authentication organisation-wide (F-01)
Give the six affected administrators a short deadline to enrol, then tick the box. 15 minutes of work.

2. Delete the personal-webmail administrator account (F-02)
It is dormant, has no second factor, holds organisation-wide full access, and is redundant. Two minutes, no operational impact.

3. Turn on malware protection and intrusion detection (F-03)
AMP on immediately; IDS/IPS in Detection mode for two weeks, then Prevention. The licences are already paid for.

4. Enable alerting and send it to a monitored address (F-07)
Configuration change, VPN up/down, rogue AP, appliance offline. Without this, none of the above is observable.

What could not be assessed

Stated so that the coverage of this report is not overstated. This assessment reads one system: the Cisco Meraki dashboard. It is therefore a strong assessment of network infrastructure security and silent on everything else.

- Threat protection and alerting were confirmed on one of ten networks. The other nine are very likely in the same state but must be verified.
- Firewall rule sets, content filtering, wireless encryption and 802.1X, switch access policies and client VPN were not read.

- No evidence outside Meraki: no endpoint protection, identity provider, backup or recovery testing, policies, risk register, supplier contracts, incident records or training records.
- Consequently the RESPOND and RECOVER functions of NIST CSF 2.0, and most of ISO 27001 Clauses 4–10 and the organisational and people controls of Annex A, are marked "not assessed" rather than compliant or non-compliant. A certification audit needs those; this report does not substitute for one.

Full findings, evidence citations and the complete NIST CSF 2.0 and ISO/IEC 27001:2022 control mapping are in the accompanying assessment report.