PUBLIC EXAMPLE — SANITISED

COMPLIANCE ASSESSMENT REPORT

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.

Contents

1. Scope, method and limitations

1.1 What was assessed

This report assesses the security configuration of Global Corp's Cisco Meraki cloud-managed network estate against the NIST Cybersecurity Framework 2.0 and the Annex A controls of ISO/IEC 27001:2022.

The estate at the assessment date:

Site	Country	Devices	Offline	Clients (7 days)
UK-1	GB	23	3	151
UK-2	GB	6	—	175
UK-3	GB	14	—	143
DE-1	DE	17	1	119
DE-2	DE	5	1	35
SE-1	SE	5	—	9
SE-2	SE	13	—	38
PL-1	PL	10	1	49
IN-1	IN	5	—	42
IN-2	IN	12	1	208
Total	**5 countries**	**110**	**7**	**969**

1.2 Method

Evidence was gathered by read-only navigation of the Cisco Meraki Dashboard using the asset owner's own authenticated session. No configuration was created, modified, deleted or saved at any point, and no Save Changes control was activated. Ten dashboard pages were read; each finding below cites the page it came from.

Where a Meraki settings page was material to a finding, the rendered control state was read from a screenshot rather than from extracted page text, because the text of a Meraki settings page lists control labels without their on/off state. This distinction matters for reproducibility and is recorded in the source register.

1.3 Limitations — read this before relying on the report

This assessment reads one system. It is a strong assessment of network infrastructure configuration and silent on everything else. Specifically:

- Threat protection (F-03) and alerting (F-07) were confirmed on one of ten networks. Both findings are reported as confirmed for that network and suspected estate-wide. Verify the remaining nine before treating them as closed — or as fixed.
- Layer-3/7 firewall rules, content filtering, group policies, per-SSID wireless encryption and 802.1X, switch access policies, port security, client VPN and Active Directory integration were not read.
- Nothing outside Meraki was examined: no endpoint protection, identity provider, backup or recovery testing, policy documents, risk register, supplier contracts, incident records or training records.

- Therefore the RESPOND and RECOVER functions of CSF 2.0, ISO 27001 Clauses 4–10 (the management system itself), and the organisational, people and physical control themes of Annex A are marked "not assessed". An ISO 27001 certification audit requires all of them. This report does not substitute for one; it removes a set of technical findings that such an audit would otherwise raise.

No penetration testing, vulnerability scanning or configuration change of any kind was performed.

2. Assessment summary

3 critical, 5 high, 5 medium and 2 low findings were identified, together with 9 confirmed strengths.

The pattern across all fifteen findings is consistent and worth stating plainly, because it determines how the remediation should be run: this is not an organisation that has failed to build a network properly. It is an organisation that has built a good network and then not switched on the protective and detective features it already owns and pays for. Twelve of the fifteen findings are closed by configuration alone. Three require coordination with a third party. None requires new hardware, new licences or new headcount.

2.1 NIST CSF 2.0 — assessment by Function

Function	Assessment	Basis
GOVERN (GV)	**Partial**	Risk-management expectations are not evidenced in platform configuration. Third-party access is extensive and ungoverned (F-08, F-12). No evidence of an access-review cadence (F-06). GV.OC-03 is supported by EU residency and privacy-by-default.
IDENTIFY (ID)	**Largely met**	Asset inventory is strong and automatic: 110 devices across 10 networks with live status. Firmware currency is visible and good. Gaps are process rather than data: no scheduled patch cadence (F-14), no evidence of risk assessment for the deprecated VPN crypto (F-04).
PROTECT (PR)	**Not met**	The weakest function. PR.AA (identity and access) fails on enforced MFA, SSO, least privilege, lockout, idle timeout and source restriction (F-01, F-02, F-05, F-06, F-10, F-11). PR.DS-02 fails on VPN cryptography (F-04). PR.PS is partially met — firmware is current, SNMP is disabled and the Cloud CLI is read-only.
DETECT (DE)	**Not met**	Logging is genuinely good; detection is absent. Change and authentication logs are detailed and retained (positive findings 1 and 2), but no alerting is enabled (F-07), AMP and IDS/IPS are off (F-03), logs never leave the platform (F-13), and an unexplained authentication anomaly went uninvestigated (F-09).
RESPOND (RS)	**Not assessed**	Cannot be assessed from platform configuration alone. One dependency is visible: without the alerting in F-07 there is no trigger to begin a response, so RS.MA-01 has no viable input today.
RECOVER (RC)	**Not assessed**	No configuration-backup, restore-testing or recovery-plan evidence is obtainable from this platform. Note that the Meraki cloud holds device configuration, which reduces but does not remove the need for a tested recovery procedure.

2.2 ISO/IEC 27001:2022 Annex A — control mapping

Only controls for which this assessment produced evidence are listed. Absence from this table means no evidence was available, not that the control is met.

Control	Title	Status	Findings
A.5.15	Access control	**Not met**	F-01, F-10, F-11
A.5.16	Identity management	**Not met**	F-01, F-02, F-05, F-06, F-08
A.5.17	Authentication information	**Not met**	F-01, F-05, F-10
A.5.18	Access rights	**Not met**	F-02, F-05, F-06, F-11
A.5.19	Information security in supplier relationships	**Not met**	F-08, F-12
A.5.20	Addressing security within supplier agreements	**Not assessed**	F-08 — contracts not reviewed
A.5.22	Monitoring and review of supplier services	**Not met**	F-08, F-12
A.5.25	Assessment and decision on security events	**Not met**	F-07, F-09
A.5.28	Collection of evidence	**Partial**	F-13 — logs exist but are not exported or protected from alteration
A.5.34	Privacy and protection of PII	**Met**	EU residency; privacy-by-default enabled
A.6.8	Information security event reporting	**Not met**	F-07
A.8.2	Privileged access rights	**Not met**	F-02, F-05, F-08, F-11, F-12
A.8.5	Secure authentication	**Not met**	F-01, F-10
A.8.7	Protection against malware	**Not met**	F-03
A.8.8	Management of technical vulnerabilities	**Partial**	F-14 — current state good, process absent
A.8.9	Configuration management	**Partial**	F-10, F-14, F-15; SNMP disabled and CLI read-only are met
A.8.15	Logging	**Partial**	Generation met and strong; protection and retention not met (F-13)
A.8.16	Monitoring activities	**Not met**	F-03, F-07, F-09, F-13
A.8.20	Networks security	**Partial**	F-03, F-04, F-15; SNMP hardening met
A.8.21	Security of network services	**Partial**	F-04
A.8.24	Use of cryptography	**Not met**	F-04 — 3 of 6 tunnels use disallowed algorithms
A.8.32	Change management	**Not met**	F-14, F-15 — log is

Control	Title	Status	Findings
			attributable but records no authority or reason

3. Findings

Each finding states the evidence it rests on, why it matters, and what closes it. Severity reflects exploitability and blast radius, not effort to fix.

F-01 — Multi-factor authentication is not enforced, and six of fourteen administrators do not use it

Severity	**Critical**	**Area**	Identity & access
NIST CSF 2.0	PR.AA-03, PR.AA-05, GV.RM-01	**ISO 27001**	A.5.15 Access control · A.5.16 Identity management · A.5.17 Authentication information · A.8.5 Secure authentication

Evidence. Organization → Settings: "Force users to set up and use two-factor authentication" is unticked. Organization → Administrators shows 2FA = Off for 6 of the 14 accounts, five of which hold Full access.

Why it matters. A single phished or reused password grants an attacker administrative control of the network in all ten countries — including the ability to alter firewall rules, create VPN tunnels, and mirror traffic. Password-only administrative access to network infrastructure is the single highest-probability path to full estate compromise, and it is also the control an insurer and an ISO 27001 auditor will look for first.

Remediation. Tick "Force users to set up and use two-factor authentication" at organisation level. Because this will lock out any admin who has not enrolled, notify the six accounts first and give a short deadline — but set the deadline in days, not weeks.

Effort: 15 minutes of configuration; 1–3 days of notice **Owner:** Group IT

F-02 — A personal consumer email address holds full organisation-wide administrative access and has been dormant for over two years

Severity	**Critical**	**Area**	Identity & access
NIST CSF 2.0	PR.AA-01, PR.AA-05, ID.AM-02	**ISO 27001**	A.5.16 Identity management · A.5.18 Access rights · A.8.2 Privileged access rights

Evidence. Organization → Administrators: one account on a public consumer webmail domain holds Role "Full access" at organisation scope, with 2FA "Off" and last activity 23 February 2024 — approximately 29 months dormant. The same individual also holds a correctly provisioned corporate account with 2FA enabled.

Why it matters. Organisation-wide administrative control of the estate rests on a mailbox the company does not own, cannot audit, cannot revoke, and cannot recover. If that mailbox is ever breached or its password reused, the attacker inherits full control — and because the account is dormant, nobody would notice the login. It is also unusable as evidence of individual accountability, since the company cannot prove who controls the mailbox.

Remediation. Delete the account. It is redundant: the same person already has a working corporate account with 2FA enabled. This is a one-click fix with no operational impact and should not wait for the next change window.

Effort: 2 minutes **Owner:** Group IT

F-03 — Malware protection and intrusion detection are switched off on the security appliances

Severity	Critical	Area	Detection
NIST CSF 2.0	DE.CM-01, DE.CM-09, PR.PS-05, DE.AE-02	ISO 27001	A.8.7 Protection against malware · A.8.16 Monitoring activities · A.8.20 Network security

Evidence. Security & SD-WAN → Threat protection, sample network DE-1: Advanced Malware Protection (AMP) Mode = Disabled. Intrusion detection and prevention Mode = Disabled. Cisco Umbrella DNS-layer protection not enabled. Cisco XDR not enabled. Organization → Settings: Cisco Secure Malware Analytics integration = Disabled.

Why it matters. The organisation owns security appliances whose security functions are turned off. Traffic crossing the perimeter is neither inspected for malware nor evaluated against intrusion signatures, and DNS requests are not filtered. There is therefore no network-layer detection capability at all: a compromise would have to be discovered by an endpoint tool, a user complaint, or the attacker's own actions. This is both the largest capability gap in the assessment and the cheapest to close, because the licences are already paid for.

Remediation. Enable IDS/IPS in Detection mode first and observe for one to two weeks to establish a false-positive baseline, then move to Prevention. Enable AMP immediately — it has minimal false-positive risk. Then repeat on all ten networks; only DE-1 was confirmed, and the others are very likely in the same state.

Effort: 1 hour per network to enable; 2 weeks of tuning before Prevention mode **Owner:** Group IT with the managed service provider

Coverage note: Confirmed on one of ten networks. Verify the remaining nine before treating this finding as closed.

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

Severity	High	Area	Cryptography
NIST CSF 2.0	PR.DS-02, PR.DS-10, PR.IR-01, ID.RA-01	ISO 27001	A.8.24 Use of cryptography · A.8.20 Network security · A.8.21 Security of network services · A.5.14 Information transfer

Evidence. Organization → Change log, IPsec peers configuration object. Of six named site-to-site tunnels: one uses IKEv1 with SHA-1 authentication and Perfect Forward Secrecy disabled; one uses IKEv2 but with SHA-1 IKE authentication, Diffie-Hellman group 2 (1024-bit MODP), an algorithm list that still accepts MD5, and PFS disabled; one uses SHA-256 and group 14 for the IKE SA but falls back to group 2 for PFS and carries an anomalous child SA lifetime of 45. The remaining three are correctly configured with IKEv2, SHA-256, group 14 and PFS group 14.

Why it matters. IKEv1 is deprecated (RFC 9395). SHA-1 and MD5 are disallowed for authentication under NIST SP 800-131A Rev. 2, and MD5 in particular is trivially collidable. 1024-bit MODP (group 2) is below the acceptable floor and within reach of a well-resourced adversary. With PFS disabled, a single compromise of the tunnel key retroactively exposes all previously captured traffic on that tunnel rather than a single

session. Two of the three affected tunnels carry traffic between the Indian sites and Azure, so the exposure is production inter-site and cloud traffic, not a lab. Three tunnels are already configured correctly, which shows the standard is known internally and simply has not been applied consistently.

Remediation. Migrate the two Indian tunnels to IKEv2 with SHA-256, DH group 14 or higher, and PFS enabled at group 14, matching the configuration already in use on the three compliant tunnels. Requires coordination with the far-end owners (the MSP and Azure). Investigate the 45-second child SA lifetime separately — it is either a typo or a cause of constant renegotiation.

Effort: 2–4 hours per tunnel including far-end coordination and a maintenance window **Owner:** Group IT with the managed service provider and the Azure team

F-05 — No single sign-on: SAML is disabled, so administrative identities are local to the dashboard and cannot be centrally revoked

Severity	High	Area	Identity & access
NIST CSF 2.0	PR.AA-01, PR.AA-03, PR.AA-05, GV.RM-01	ISO 27001	A.5.16 Identity management · A.5.17 Authentication information · A.5.18 Access rights · A.8.2 Privileged access rights

Evidence. Organization → Administrators → SAML: "SAML is disabled on this organization". Organization → Settings → Authentication: SAML SSO = "SAML SSO disabled". No RADIUS servers are defined at organisation level ("No matches found").

Why it matters. Every administrator is a standalone local account. A leaver disabled in the corporate directory keeps working access to the network estate until somebody remembers to delete them here as well — and the dormant accounts in F-06 are the evidence that this does not reliably happen. It also means no conditional access, no device-trust requirement, no central session policy, and no single place to prove to an auditor who has access to what.

Remediation. Enable SAML SSO against the corporate identity provider and map SAML groups to Meraki roles. Retain exactly one break-glass local account with a long unique passphrase, 2FA enrolled, and its credentials held under change control. Then remove the remaining local admins.

Effort: 1–2 days including testing and the break-glass procedure **Owner:** Group IT / identity team

F-06 — Dormant administrator accounts are not removed; access rights are not reviewed

Severity	High	Area	Identity & access
NIST CSF 2.0	PR.AA-01, PR.AA-05, ID.AM-02, GV.RR-02	ISO 27001	A.5.18 Access rights · A.5.16 Identity management · A.8.2 Privileged access rights

Evidence. Organization → Administrators, last-active dates: four accounts holding Full access have been dormant for approximately 29, 24, 24 and 8 months respectively. Two of the four also have 2FA disabled. There is no evidence of a periodic access review.

Why it matters. Four unused sets of administrative credentials remain valid. Dormant privileged accounts are attractive precisely because nobody is watching them — an anomalous login on an account in daily use may be noticed, whereas one on an account unused since 2024 will not. Two of these belong to a supplier

whose engagement status is not evidenced anywhere in the dashboard, so it is not even clear whether the access is still contractually justified.

Remediation. Delete the four dormant accounts now. Then institute a quarterly access review of the administrator list — the dashboard's own last-active column and CSV export make this a fifteen-minute task, and the review record is itself the ISO 27001 A.5.18 evidence.

Effort: 30 minutes now; 15 minutes per quarter thereafter **Owner:** Group IT

F-07 — No alerting is enabled: configuration changes, VPN failures, rogue access points and appliance outages generate no notification

Severity	High	Area	Detection
NIST CSF 2.0	DE.AE-02, DE.AE-03, DE.CM-01, DE.CM-03, RS.MA-01	ISO 27001	A.8.16 Monitoring activities · A.8.15 Logging · A.5.25 Assessment and decision on information security events · A.6.8 Information security event reporting

Evidence. Network-wide → Alerts, sample network DE-1: every alert checkbox is unticked, including "Configuration settings are changed", "A VPN connection comes up or goes down", "A rogue access point is detected", "A WAN appliance goes offline" and "The primary uplink status changes". Default recipients are two individual mailboxes rather than a monitored team address. Organization → Login attempts: SNMP Trap Subscription Status = Disabled.

Why it matters. The platform records events well (see the positive findings) but tells nobody about them. An attacker who obtains admin access can change firewall rules, stand up a new VPN tunnel, or bring a site down and generate no notification whatsoever — detection depends entirely on somebody choosing to open the change log. "A rogue access point is detected" being off is a particular gap for a manufacturer with physical sites. The two named recipients are also a single-point-of-failure: if both are on leave, alerts (once enabled) reach nobody.

Remediation. Enable at minimum: configuration settings changed, VPN connection up/down, rogue AP detected, WAN appliance offline, primary uplink status change. Replace the two personal mailboxes with a monitored group address, and add the MSP's service desk. Repeat on all ten networks.

Effort: 30 minutes per network **Owner:** Group IT with the managed service provider

Coverage note: Confirmed on one of ten networks.

F-08 — Five external parties hold administrative access, one via a shared generic account used from two countries

Severity	High	Area	Third-party risk
NIST CSF 2.0	GV.SC-04, GV.SC-07, GV.SC-09, PR.AA-01, PR.AA-05	ISO 27001	A.5.19 Information security in supplier relationships · A.5.20 Addressing information security within supplier agreements · A.5.22 Monitoring, review and change management of supplier services · A.8.2 Privileged access rights · A.5.16 Identity management

Evidence. Organization → Administrators: five distinct external supplier domains hold administrative access, accounting for 8 of the 14 administrator accounts. One supplier holds four separate Full access accounts. One supplier account is a shared role mailbox rather than a named individual, and Organization → Login attempts shows it authenticating from two different countries. One external Full access account has 2FA disabled.

Why it matters. More than half of all administrative access to the network estate belongs to organisations other than the asset owner, and the largest single block of Full access accounts belongs to one supplier. The shared role account is the sharper problem: actions taken through it cannot be attributed to a person, which defeats accountability, breaks the audit trail's evidential value, and means credential rotation on staff turnover at the supplier is invisible to the asset owner. Two countries of origin on one shared account is consistent with legitimate follow-the-sun operations, but it is indistinguishable from credential sharing or compromise using the evidence available.

Remediation. Reduce each supplier to the minimum role its contract requires — several of these should be Observer or a limited role rather than Full access. Replace the shared role account with named individual accounts. Obtain written confirmation from each supplier of who holds access and why, and add supplier access to the quarterly review in F-06.

Effort: 1 day of review plus supplier correspondence **Owner:** Group IT and procurement / vendor management

F-09 — Repeated two-factor authentication failures on a shared supplier account are not investigated

Severity	Medium	Area	Identity & access
NIST CSF 2.0	DE.CM-01, DE.CM-03, DE.AE-02, ID.RA-01	ISO 27001	A.8.16 Monitoring activities · A.5.25 Assessment and decision on information security events · A.8.15 Logging

Evidence. Organization → Login attempts, a five-day window: at least thirteen "Two Factor Auth Failure" events on a single shared supplier account from one source address, each closely preceded or followed by a "Login Success" from the same address — in one case a failure and a success one second apart.

Why it matters. The most likely explanation is benign: a shared time-based one-time-password seed used by several engineers, with clock skew or copy-paste errors producing failures. But that benign explanation is itself a control weakness, because it means a single TOTP seed is shared among people. The pattern is also consistent with an attacker in possession of the password attempting second-factor bypass alongside legitimate sessions, and nothing in the current configuration would distinguish the two — there is no alerting (F-07) and no lockout (F-10). It requires investigation, and it is reported here as unexplained rather than as an incident.

Remediation. Ask the supplier to explain the pattern in writing. Replace the shared account with named accounts each holding its own second factor (see F-08). Enable account lockout (F-10) so repeated second-factor failure has a consequence.

Effort: 2 hours of investigation **Owner:** Group IT

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

Severity	Medium	Area	Identity & access

NIST CSF 2.0	PR.AA-03, PR.AA-05, PR.PS-01, PR.IR-01	**ISO 27001**	A.5.15 Access control · A.5.17 Authentication information · A.8.5 Secure authentication · A.8.9 Configuration management

Evidence. Organization → Settings, all unticked: "Lock accounts after N consecutive failed login attempts"; "Logout users after N minutes of inactivity"; "Force users to set passwords with a minimum of 8 characters"; "Force users to increase minimum password length to 12 characters"; "Allow Dashboard and Dashboard API access to these IP ranges"; "Allow Dashboard API access to these IP ranges". The only enabled control in the section is password history, set to 2. Password expiry is off — which is correct and deliberate under NIST SP 800-63B, and is not reported as a finding.

Why it matters. Online password guessing against the dashboard is unthrottled: there is no lockout, and combined with the absence of enforced MFA (F-01) that is a viable attack rather than a theoretical one. No idle timeout means an unattended authenticated browser session stays live indefinitely. No minimum length means an administrator may legitimately be using a short password today. Leaving both the dashboard and its API reachable from any source address forgoes the single most effective compensating control available on this platform, and the API matters more than the UI, because API access is programmatic and unattended.

Remediation. Set account lockout to 5 attempts, idle timeout to 30 minutes, and minimum password length to 12 characters. Restrict Dashboard API access to the corporate and MSP egress ranges — start with API-only, which is lower-risk than restricting the UI, and extend to the UI once the necessary ranges are confirmed. Do not enable forced password expiry.

Effort: 30 minutes for the account controls; 1 day to enumerate egress ranges before applying IP restriction **Owner:** Group IT

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

Severity	**Medium**	**Area**	Identity & access
NIST CSF 2.0	PR.AA-05, GV.RR-02	**ISO 27001**	A.5.15 Access control · A.5.18 Access rights · A.8.2 Privileged access rights

Evidence. Organization → Administrators → Roles: Full access / "All settings within an organization" = 10 accounts; Full access / "All settings within a network" = 4; Observer / organisation = 4; Observer / network = 0. Of the five available limited roles (Switch port manager, SSID manager, Client monitor, Guest ambassador, Camera footage & sensor), none is in use, and no custom roles have been created.

Why it matters. Ten accounts can change any setting in any country, including deleting networks, altering firewall policy and disabling logging. Several of these accounts plainly do not need that scope — a supplier engaged for one site's switching does not need organisation-wide authority over the German and Indian sites. Uniform maximum privilege also removes any meaningful separation of duties and enlarges the blast radius of every one of the credential findings above.

Remediation. Right-size each account against what it actually does, using the limited roles and per-network scoping the platform already provides. The last-active and change-log data give an evidence base for what each account genuinely uses. Fold this into the SAML group mapping in F-05 so it is enforced by the identity provider rather than by hand.

Effort: 1 day of analysis and reassignment **Owner:** Group IT

F-12 — Cisco support is permitted standing full access to the organisation

Severity	Medium	Area	Vendor access
NIST CSF 2.0	GV.SC-04, GV.SC-07, PR.AA-05	ISO 27001	A.5.19 Information security in supplier relationships · A.5.22 Monitoring, review and change management of supplier services · A.8.2 Privileged access rights

Evidence. Organization → Settings → Meraki Support Access: "Full access – Allow Meraki Support access to this organization to troubleshoot issues" is selected, rather than "Blocked".

Why it matters. The vendor can enter the organisation and change configuration without a per-incident authorisation step. This is a common and often reasonable operational choice — it shortens support cases materially — but it is standing rather than just-in-time third-party privileged access, and an ISO 27001 auditor will expect either a documented risk acceptance or a just-in-time model. Left undocumented it is a finding; documented, it is a decision.

Remediation. Either set it to Blocked and enable it only for the duration of an open support case, or record a formal risk acceptance referencing the Cisco support agreement. Both are defensible; silence is not.

Effort: 1 hour to document, or 2 minutes to change **Owner:** Group IT / CISO

F-13 — Logs are generated but never leave the platform: no syslog or SIEM export, and retention is bounded by the vendor

Severity	Medium	Area	Logging
NIST CSF 2.0	PR.PS-04, DE.AE-03, DE.AE-06, ID.AM-08	ISO 27001	A.8.15 Logging · A.8.16 Monitoring activities · A.5.28 Collection of evidence

Evidence. Organization → Change log holds 2,495 changes dating back to 6 August 2025 — approximately 12 months. Packet capture entries show "Automatically deleted due to 90 day retention policy". Organization → Login attempts holds 1,406 entries. No syslog server, no SIEM integration and no SNMP trap subscription were found; SNMP v2c and v3 are both disabled at organisation level, and the login-attempt trap subscription is explicitly Disabled.

Why it matters. Two consequences. First, correlation: network events cannot be joined to endpoint, identity or application events, so an investigation has to be run by hand in three consoles. Second, and more serious for an auditor, custody and retention: the only copy of the audit trail is held by the vendor under the vendor's retention policy, and an administrator with Full access — of which there are ten — is not prevented from acting inside the window and relying on eventual expiry. ISO 27001 A.8.15 expects logs to be protected against alteration; a log that only exists in the system being audited is weakly protected.

Remediation. Configure syslog export to the corporate SIEM, or if there is no SIEM, to any write-once collector. Enable the SNMP trap subscription for login attempts. Set a documented retention period that meets the organisation's own policy and any regulatory obligation, and verify the export by reconciling a known change against the collector.

Effort: 1–2 days depending on whether a collector already exists **Owner:** Group IT / SOC

F-14 — Firmware is current but patching is reactive: no maintenance window is scheduled and one platform is a release behind

Severity	Low	Area	Vulnerability management
NIST CSF 2.0	ID.RA-01, PR.PS-02, ID.AM-08	ISO 27001	A.8.8 Management of technical vulnerabilities · A.8.9 Configuration management · A.8.32 Change management

Evidence. Organization → Firmware upgrades: 0 networks at WARNING, 0 at CRITICAL — the estate is in good shape. However "Scheduled changes: There are no scheduled changes". Most recent activity was three batches approximately two months ago. Cameras run MV 7.2.1 while the current release is MV 7.3.1 (13 July 2026). Switches, security appliances and access points are on current recommended releases.

Why it matters. The outcome is currently good, but it is achieved by someone remembering rather than by a process, and that is what an auditor will test. With no scheduled window, the time-to-patch for the next critical Meraki advisory is unbounded and depends on individual attention. The camera platform being one release behind is low-risk in itself but is the visible symptom of the absent process.

Remediation. Define and schedule a recurring maintenance window per platform, using the dashboard's own scheduled-change feature so the schedule is itself the evidence. Bring the camera platform to MV 7.3.1 at the next window. Document the patch SLA — for example, critical advisories within 14 days.

Effort: 2 hours to define and schedule **Owner:** Group IT with the managed service provider

F-15 — Ad-hoc configuration changes without evidence of change control, including a protective switch feature being disabled

Severity	Low	Area	Configuration management
NIST CSF 2.0	PR.PS-01, ID.AM-08, GV.RR-02	ISO 27001	A.8.9 Configuration management · A.8.32 Change management · A.8.20 Network security

Evidence. Organization → Change log: at one Indian site, STP BPDU guard was changed from enabled to disabled on a switch port (loop guard was enabled in its place). At a Swedish site, several ports were moved between access and trunk mode with native VLAN 1. At a UK site, uplink bandwidth limits were raised from 100 Mbps to 1000 Mbps. Every entry carries an administrator name and timestamp, but no change reference, no approval and no stated reason.

Why it matters. The change log is genuinely good raw material — attributable and timestamped — but it records what changed, not why or on whose authority, so it cannot evidence a change management process to an auditor. The BPDU guard change is the one to look at on its merits: disabling it removes protection against a rogue switch or a loop introduced at an access port, and while enabling loop guard covers part of the same ground, it is a different control with a different failure mode. Trunk ports carrying native VLAN 1 is a long-standing hardening anti-pattern.

Remediation. Require a change reference in the change note for any configuration change, so the dashboard log and the change record can be reconciled. Review the BPDU guard change on its technical merits and revert if it was made for convenience. Move trunk native VLANs off VLAN 1.

Effort: 4 hours of review; process change ongoing **Owner:** Group IT with the managed service provider

4. What is already compliant

These are recorded with the same rigour as the findings, for three reasons. They are evidence an auditor can use. They show which internal standards already exist and simply need applying consistently — F-04 is the clearest example, since three tunnels are already correct. And an assessment that reports only failures gives a false picture of an estate that is, in most technical respects, well run.

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. Many organisations cannot produce this for their network estate at all. It satisfies the generation half of ISO 27001 A.8.15 and NIST DE.AE-03, and it is what made several findings in this report provable rather than suspected.

NIST CSF 2.0: DE.AE-03, PR.PS-04 **ISO 27001:** A.8.15

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. This is above the level of detail most platforms provide and directly supports NIST DE.CM-01.

NIST CSF 2.0: DE.CM-01, DE.CM-03 **ISO 27001:** A.8.15, A.8.16

EU data residency

Organisation data is hosted in Europe, as stated by the platform. This materially simplifies the GDPR Chapter V position on international transfers for the network telemetry held in the platform.

NIST CSF 2.0: GV.OC-03, ID.AM-08 **ISO 27001:** A.5.34, A.8.10

Legacy SNMP is fully disabled

Both SNMP v2c and SNMP v3 are disabled at organisation level. SNMP v2c in particular transmits its community string in clear text and is a routine finding elsewhere; its absence here is a deliberate hardening decision worth crediting.

NIST CSF 2.0: PR.PS-01, PR.IR-01 **ISO 27001:** A.8.9, A.8.20, A.8.24

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. This is correct least-privilege applied to a powerful interface.

NIST CSF 2.0: PR.AA-05, PR.PS-01 **ISO 27001:** A.8.2, A.8.9

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. Privacy by default is explicitly what GDPR Article 25 asks for, and configuring it at the platform level rather than per site is the right place to do it.

NIST CSF 2.0: GV.OC-03, PR.DS-01 **ISO 27001:** A.5.34, A.8.11

Firmware across the estate is current, with no networks in a warning or critical state

Zero of ten networks are flagged WARNING or CRITICAL, and switches, security appliances and access points all run current recommended releases. The process gap in F-14 is real, but the present technical state is good and should not be mistaken for neglect.

NIST CSF 2.0: ID.RA-01, PR.PS-02 **ISO 27001:** A.8.8

Three of six site-to-site VPN tunnels already meet current cryptographic guidance

The Azure VWAN hub tunnel and both German tunnels use IKEv2 with SHA-256, DH group 14 and PFS at group 14. This matters beyond the three tunnels: the correct standard is evidently known inside the organisation, so F-04 is a consistency failure rather than a knowledge gap, and the fix is to apply an existing internal pattern.

NIST CSF 2.0: PR.DS-02, PR.DS-10 **ISO 27001:** A.8.24

Password expiry is correctly left disabled

Forced periodic password expiry is off. This is deliberately listed as a positive rather than a gap: NIST SP 800-63B advises against arbitrary rotation because it drives predictable password mutation, and an assessor citing it as a finding would be applying superseded guidance. Password history is enabled.

NIST CSF 2.0: PR.AA-03 **ISO 27001:** A.5.17, A.8.5

5. Remediation plan

Sequenced so that each stage makes the next one observable. Enabling detection before hardening identity would mean watching an open door; hardening identity without detection would mean not knowing whether it worked.

Stage 1 — within 7 days: close the critical findings

Under one working day of configuration. The notice period for MFA enrolment, not the work, sets the timeline.

- F-01 Enforce MFA organisation-wide, after short notice to the six affected accounts.
- F-02 Delete the personal-webmail full-access account. No operational impact; it is redundant.
- F-03 Enable AMP now; enable IDS/IPS in Detection mode. Do this on all ten networks, not just the one sampled.
- F-07 Enable the core alerts and point them at a monitored group mailbox plus the service desk.
- F-06 Delete the four dormant full-access accounts.

Stage 2 — within 30 days: remove the standing exposure

- F-10 Account lockout at 5 attempts, idle timeout at 30 minutes, minimum password length 12. Then restrict Dashboard API access by source range — API first, UI once ranges are confirmed.
- F-04 Migrate the two non-compliant tunnels to IKEv2 / SHA-256 / DH group 14 / PFS group 14, matching the three tunnels already configured correctly. Investigate the 45-second child SA lifetime.
- F-08 Right-size supplier access, replace the shared role account with named accounts, and obtain written confirmation of who holds access and why.
- F-09 Obtain a written explanation of the repeated second-factor failures.
- F-03 Move IDS/IPS from Detection to Prevention once the false-positive baseline is established.

Stage 3 — within 90 days: make it structural

- F-05 Enable SAML SSO against the corporate identity provider, map groups to roles, retain one controlled break-glass account, remove the remaining local admins.
- F-11 Apply least privilege using the platform's limited roles and per-network scoping, enforced through the SAML group mapping.
- F-13 Export logs to a SIEM or write-once collector, enable the login-attempt trap subscription, set and document a retention period, and verify by reconciling a known change.
- F-14 Schedule recurring firmware windows per platform and document the patch SLA. Bring cameras to the current release.
- F-12 Either set Cisco support access to Blocked and grant it per incident, or record a formal risk acceptance.
- F-15 Require a change reference on every configuration change; review the BPDU guard change on its merits; move trunk native VLANs off VLAN 1.

Ongoing

- Quarterly review of the administrator list, including supplier accounts, using the dashboard's last-active data and CSV export. The review record is itself the ISO 27001 A.5.18 evidence.
- Re-run this assessment after Stage 1 and again after Stage 3, to evidence the change rather than assert it.

99. Source register and reproducibility

99.1 Primary source

Platform	Cisco Meraki Dashboard
Dashboard shard	(redacted)
Organisation	Global Corp (real name withheld)
Data residency	Europe
Collection date	26–27 July 2026 (Europe/Stockholm)
Access used	The asset owner's own authenticated dashboard session, on the asset owner's own workstation
Change made	None. Read-only navigation throughout.

99.2 Dashboard pages read

#	Page	Evidence taken
S1	Organization → Overview	Network inventory, per-site device/client counts, offline counts
S2	Organization → Administrators → Admins	14 accounts: role, scope, last active, 2FA state
S3	Organization → Administrators → Roles	Role distribution; no custom roles in use
S4	Organization → Administrators → SAML	SAML disabled
S5	Organization → Settings	Authentication and security posture, SNMP, vendor access, privacy, Cloud CLI
S6	Organization → Login attempts	1,406 attempts with source IP, geolocation, outcome; trap subscription state
S7	Organization → Change log	2,495 changes from 2025-08-06, including full IPsec peer objects
S8	Organization → Firmware upgrades	Installed vs latest per platform; scheduled-change queue
S9	Security & SD-WAN → Threat protection (1 network)	AMP, IDS/IPS, Umbrella, XDR state
S10	Network-wide → Alerts (1 network)	Alert recipients and per-event enablement

99.3 Standards and guidance relied on

- NIST Cybersecurity Framework 2.0 — NIST CSWP 29, February 2024. Primary assessment structure.
- ISO/IEC 27001:2022 Annex A, with ISO/IEC 27002:2022 for implementation guidance. Control mapping.
- NIST SP 800-63B — basis for treating forced password expiry as unnecessary and MFA as required.

- NIST SP 800-131A Rev. 2 — basis for classifying SHA-1, MD5 and 1024-bit MODP as disallowed.
- NIST SP 800-77 Rev. 1 — IPsec VPN configuration guidance underlying F-04.
- RFC 9395 (IKEv1 deprecation) and RFC 8247 (IKEv2 algorithm requirements).

99.4 Reproducing this assessment

Every finding names the dashboard page it was read from, so it can be re-derived by opening that page. To reproduce systematically rather than by hand, the same evidence is available through the Meraki Dashboard API — the relevant endpoints are:

- GET /organizations/{orgId}/admins — F-01, F-02, F-06, F-08, F-11
- GET /organizations/{orgId} and …/saml — F-05, F-10, F-12
- GET /organizations/{orgId}/loginSecurity — F-01, F-10
- GET /organizations/{orgId}/configurationChanges — F-04, F-15, and the audit-trail positive finding
- GET /organizations/{orgId}/apiRequests and …/devices/statuses — inventory and F-14
- GET /networks/{netId}/appliance/security/intrusion and …/malware — F-03
- GET /networks/{netId}/alerts/settings — F-07
- GET /networks/{netId}/appliance/vpn/siteToSiteVpn and …/thirdPartyVPNPeers — F-04

Running those nine endpoint families against the organisation reproduces every finding in this report without a browser, which is the intended path for re-assessment after remediation.

Report generated 26 July 2026 by Objektiv AI — Claude Opus 5 (Anthropic). Machine-generated from read-only inspection of the organisation's own cloud management platform and from the public standards listed in section 99.3.

This is a sanitised public example. The organisation has been renamed, and site names, personal names, email addresses, IP addresses, MAC addresses, device serial numbers and network subnets have been removed or generalised. Findings, severities, control mappings and reasoning are unchanged from the internal report.