

Sample deliverable

Sample: Monthly Security Leadership Report

Sample document. All findings, scores, account identifiers, and company details are fictional demonstration data created to show report format and depth. This is not a real client engagement.

CLIENT	REPORTING PERIOD	ENGAGEMENT MONTH	HOURS USED
Cordova Technologies (sample)	March 2026	7	19.5 of 20

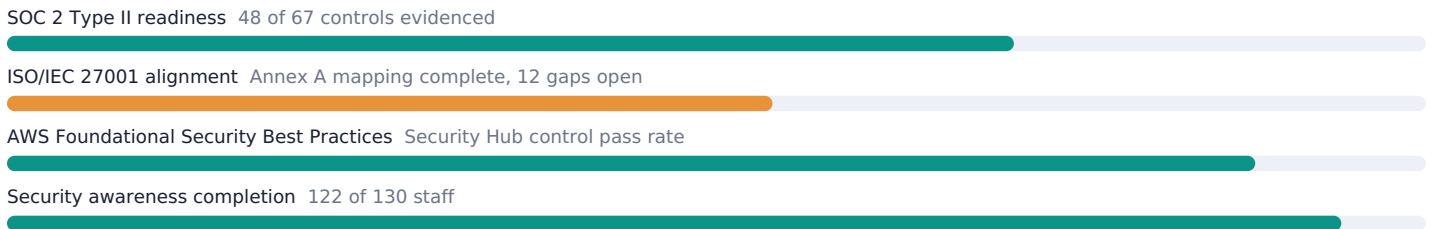
Posture at a glance

B Posture improved four points this month, driven by closing the last two High findings from the January Security Hub baseline and completing MFA enforcement across all human access. SOC 2 readiness advanced to 71%.

82 / 100 · up 4 pts

One item needs a decision from leadership: the exception request for the legacy reporting server, which cannot support the agent required by the endpoint standard. Options and a recommendation are on page 2.

Compliance progress



Open risks

ID	RISK	SEVERITY	OWNER	TREATMENT	STATUS
R-14	Legacy reporting server cannot run the required endpoint agent	High	CTO	Exception requested, compensating controls proposed	Decision needed
R-09	Single administrator for the production AWS Organization	High	Cloud Lead	Second admin onboarding, break-glass documented	In progress
R-11	Vendor SOC 2 reports not collected for four critical suppliers	Medium	vCISO	Requests issued, two received	In progress
R-17	Backup restore testing not performed in 2026	Medium	IT Manager	Restore test scheduled for April	Scheduled
R-18	Terraform state bucket versioning disabled	Low	Cloud Lead	Remediated 18 Mar	Closed

Vulnerability management

SEVERITY	OPEN	OPENED THIS MONTH	CLOSED THIS MONTH	OLDEST OPEN	WITHIN SLA
Critical	0	1	1	—	Yes
High	3	7	9	19 days	Yes
Medium	24	18	14	64 days	No — 6 past 60-day SLA

						SLA
Low	71	22	9	180+ days	Not tracked to SLA	

Decision required: endpoint standard exception

Request. The legacy reporting server (Windows Server 2016, hosting the warehouse analytics database) cannot run the required EDR agent without vendor-confirmed instability. Engineering has requested a 12-month exception.

Options.

- **Grant with compensating controls** — network isolation in a dedicated subnet, host-based firewall restricting inbound to two application servers, weekly log review, and quarterly re-evaluation. Residual risk: medium. Cost: ~3 engineering days.
- **Accelerate migration** — the application is scheduled for replacement in Q1 2027. Pulling it forward removes the risk entirely. Cost: significant, and it displaces roadmap work.
- **Deny** — forces agent installation against vendor guidance, with an availability risk to a system used in daily operations.

Recommendation. Grant the exception with compensating controls and a hard expiry at the migration date, documented in the risk register with CTO sign-off. This keeps the SOC 2 narrative defensible, since auditors accept documented exceptions with compensating controls far more readily than undocumented deviations.

Activity this month

AREA	WORK COMPLETED	HOURS
Program	Q2 roadmap re-sequenced after the SOC 2 timeline moved up; risk register reviewed with the CTO	3.5
Policy	Endpoint standard and exception procedure finalized; access control policy updated for IAM Identity Center	4.0
Compliance	Evidence collection for 11 SOC 2 controls; Audit Manager assessment configured	5.0
Vendor risk	Four supplier reviews initiated, two completed with findings documented	2.5
Operations	Security Hub findings triage, MFA enforcement verification, backup test scheduling	3.0
Stakeholder	Engineering office hours, exception review with the CTO, board deck preparation	1.5

Next month

- Close the remaining six Medium findings past the 60-day SLA, or document accepted exceptions
- Complete the backup restore test and capture evidence for SOC 2 CC9.1
- Finish the remaining two vendor reviews and add Marketplace Vendor Insights evidence where available
- Draft the Q2 board readout, covering posture trend, exception decisions, and SOC 2 timeline confidence

About this report. Produced monthly as part of the fractional security leadership engagement, drawn from AWS Security Hub, GuardDuty, Inspector, Audit Manager, and the maintained risk register. The quarterly executive readout summarizes three months of this data for the board.