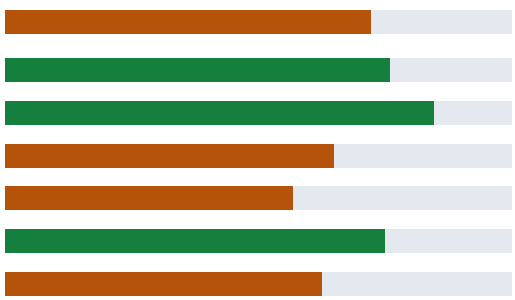
Your vCISO Practice

Security Posture Report

Northwind Dental

Framework: NIST Cybersecurity Framework 2.0
Generated: 2026-10-17

Posture summary



Gap analysis

Findings: 23 (critical 2, high 8, medium 13, low 0)

[CRITICAL] PR.DS-02: Gap on PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected (status: not_implemented)
[CRITICAL] PR.PS-01: Gap on PR.PS-01: Configuration management practices are established and applied (status: not_implemented)
[HIGH] GV.SC-03: Gap on GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (status: not_implemented)
[HIGH] GV.SC-10: Gap on GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement (status: not_implemented)
[HIGH] PR.AA-01: Gap on PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization (status: partially)
[HIGH] PR.AT-02: Gap on PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind (status: not_implemented)
[HIGH] PR.DS-01: Gap on PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected (status: partially)
[HIGH] DE.AE-03: Gap on DE.AE-03: Information is correlated from multiple sources (status: not_implemented)
[HIGH] DE.AE-08: Gap on DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria (status: not_implemented)
[HIGH] RC.RP-02: Gap on RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed (status: not_implemented)
[MEDIUM] GV.OC-03: Gap on GV.OC-03: Legal, regulatory, and contractual requirements regarding

cybersecurity - including privacy and civil liberties obligations - are understood and managed (status: partially)
[MEDIUM] GV.OC-05: Gap on GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated (status: partially)
[MEDIUM] GV.RM-07: Gap on GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions (status: partially)
[MEDIUM] GV.SC-06: Gap on GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships (status: partially)
[MEDIUM] ID.RA-10: Gap on ID.RA-10: Critical suppliers are assessed prior to acquisition (status: partially)
[MEDIUM] PR.IR-02: Gap on PR.IR-02: The organization's technology assets are protected from environmental threats (status: partially)
[MEDIUM] DE.CM-03: Gap on DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events (status: partially)
[MEDIUM] DE.CM-09: Gap on DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (status: partially)
[MEDIUM] DE.AE-07: Gap on DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis (status: partially)
[MEDIUM] RS.CO-02: Gap on RS.CO-02: Internal and external stakeholders are notified of incidents (status: partially)
[MEDIUM] RS.CO-03: Gap on RS.CO-03: Information is shared with designated internal and external stakeholders (status: partially)
[MEDIUM] RC.RP-06: Gap on RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed (status: partially)
[MEDIUM] RC.CO-03: Gap on RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders (status: partially)

Prioritized remediation roadmap

1. Enforce MFA on the practice management system, email and remote access [status: in_progress, effort: medium]
2. Encrypt and test restores of the nightly imaging and patient-record backups [status: open, effort: medium]
3. Build and maintain an inventory of workstations, imaging devices and cloud apps [status: in_progress, effort: low]
4. Write and tabletop-test an incident response plan with the office manager [status: open, effort: medium]
5. Turn on centralized logging and alerting for the EHR and firewall [status: open, effort: high]
6. Review vendor access for the dental software and IT support providers [status: open, effort: low]
7. Run quarterly access reviews and remove departed staff accounts [status: done, effort: low]

Evidence status

Requests: 14, submitted: 5, accepted: 6