

# Sample Dental Group (made up)

Reassessment: what changed · NIST CSF 2.0 · Jan 23, 2026 to Oct 16, 2026

## KEY FACTS

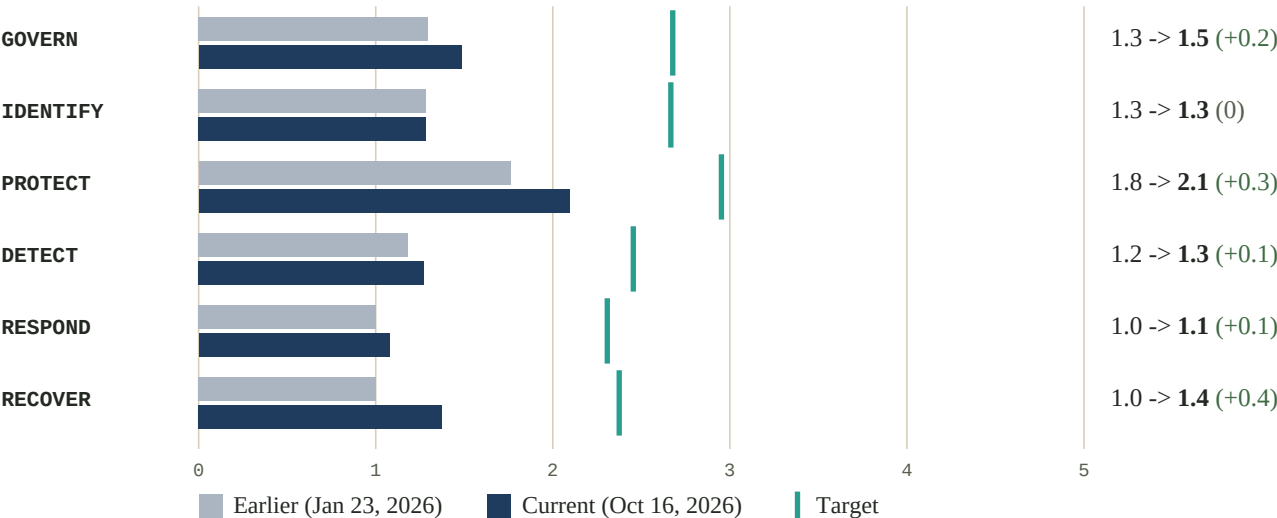
|                                                                                    |                                                       |                                        |                                                                                                                               |
|------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <div>Jan 23, 2026</div> <div>EARLIER ASSESSMENT</div>                              | <div>Oct 16, 2026</div> <div>CURRENT ASSESSMENT</div> | <div>9</div> <div>MONTHS BETWEEN</div> | <div>1.3 -&gt; 1.4</div> <div>OVERALL MATURITY (0 TO 5)</div> <div>Up 0.1 since the January 2026 assessment. Target 2.6</div> |
| <div>11</div> <div>GAPS CLOSED</div> <div>of 97 found last time; 92 open now</div> | <div>2</div> <div>RISKS CLOSED</div>                  | <div>1</div> <div>NEW RISKS</div>      | <div>1 -&gt; 1</div> <div>CSF TIER</div> <div>Target Tier 2</div>                                                             |

## SUMMARY

Most of the progress came from the security policy being approved and signed, laptops being encrypted, backups now tested every quarter and MFA reaching 11 of 14 mailboxes. The two declines are housekeeping that slipped as the IT provider changed engineers: the device list and the firewall firmware. The next nine months are about network separation, log collection and a tested incident response plan.

Over 9 months between the two assessments, the average maturity rating moved from 1.3 to 1.4 out of 5, against a target of 2.6. 18 subcategories improved, 81 stayed the same and 2 declined; 4 were assessed for the first time. 11 of the 97 gaps found last time have reached their target.

## MATURITY BY FUNCTION



| Function       | Earlier    | Current    | Change      | Target     | Still to go |
|----------------|------------|------------|-------------|------------|-------------|
| Govern         | 1.3        | 1.5        | +0.2        | 2.7        | 1.2         |
| Identify       | 1.3        | 1.3        | 0           | 2.7        | 1.4         |
| Protect        | 1.8        | 2.1        | +0.3        | 3.0        | 0.9         |
| Detect         | 1.2        | 1.3        | +0.1        | 2.5        | 1.2         |
| Respond        | 1.0        | 1.1        | +0.1        | 2.3        | 1.2         |
| Recover        | 1.0        | 1.4        | +0.4        | 2.4        | 1.0         |
| <b>Overall</b> | <b>1.3</b> | <b>1.4</b> | <b>+0.1</b> | <b>2.6</b> | <b>1.1</b>  |

Scores are the consultant's maturity ratings for each subcategory, from 0 (not performed) to 5 (optimized), averaged within each function. They describe how established each practice is; they are not a certification, an audit opinion or a prediction of any insurance outcome. CSF tier: Tier 1 (Partial) then, Tier 1 (Partial) now.

## BIGGEST IMPROVEMENTS

| Subcategory                                                                                                                                                                                                                                                   | Earlier | Current | Change |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|--------|
| GV.PO-01 Policy<br>Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced                                                                            | 1       | 3       | +2     |
| PR.DS-01 Data Security<br>The confidentiality, integrity, and availability of data-at-rest are protected                                                                                                                                                      | 1       | 3       | +2     |
| RC.RP-03 Incident Recovery Plan Execution<br>The integrity of backups and other restoration assets is verified before using them for restoration                                                                                                              | 1       | 3       | +2     |
| GV.OC-03 Organizational Context<br>Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed                                                                   | 2       | 3       | +1     |
| GV.RR-02 Roles, Responsibilities, and Authorities<br>Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced                                                                | 1       | 2       | +1     |
| GV.RR-04 Roles, Responsibilities, and Authorities<br>Cybersecurity is included in human resources practices                                                                                                                                                   | 2       | 3       | +1     |
| GV.PO-02 Policy<br>Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission                                                               | 1       | 2       | +1     |
| GV.SC-05 Cybersecurity Supply Chain Risk Management<br>Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties | 2       | 3       | +1     |
| ID.AM-08 Asset Management<br>Systems, hardware, software, services, and data are managed throughout their life cycles                                                                                                                                         | 1       | 2       | +1     |
| PR.AA-03 Identity Management, Authentication, and Access Control<br>Users, services, and hardware are authenticated                                                                                                                                           | 1       | 2       | +1     |
| PR.AA-05 Identity Management, Authentication, and Access Control<br>Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties | 1       | 2       | +1     |
| PR.AA-06 Identity Management, Authentication, and Access Control<br>Physical access to assets is managed, monitored, and enforced commensurate with risk                                                                                                      | 2       | 3       | +1     |

| Subcategory                                                                                                                                                                                   | Earlier | Current | Change |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|--------|
| PR.AT-01 Awareness and Training<br>Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind | 2       | 3       | +1     |
| PR.DS-11 Data Security<br>Backups of data are created, protected, maintained, and tested                                                                                                      | 2       | 3       | +1     |
| PR.PS-02 Platform Security<br>Software is maintained, replaced, and removed commensurate with risk                                                                                            | 2       | 3       | +1     |

And 3 more, each up by one level.

## DECLINES

| Subcategory                                                                                        | Earlier | Current | Assessor's note now                                                             |
|----------------------------------------------------------------------------------------------------|---------|---------|---------------------------------------------------------------------------------|
| ID.AM-01 Asset Management<br>Inventories of hardware managed by the organization are maintained    | 3       | 2       | IT provider keeps a device list; two imaging workstations were missing from it. |
| PR.PS-03 Platform Security<br>Hardware is maintained, replaced, and removed commensurate with risk | 3       | 2       | Firewall firmware two releases behind.                                          |

## GAPS CLOSED

| Subcategory                                                                                                                                                                                                                                                   | Earlier | Current | Target |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|--------|
| GV.OC-03 Organizational Context<br>Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed                                                                   | 2       | 3       | 3      |
| GV.RR-04 Roles, Responsibilities, and Authorities<br>Cybersecurity is included in human resources practices                                                                                                                                                   | 2       | 3       | 3      |
| GV.PO-01 Policy<br>Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced                                                                            | 1       | 3       | 3      |
| GV.SC-05 Cybersecurity Supply Chain Risk Management<br>Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties | 2       | 3       | 3      |
| PR.AA-06 Identity Management, Authentication, and Access Control<br>Physical access to assets is managed, monitored, and enforced commensurate with risk                                                                                                      | 2       | 3       | 3      |
| PR.AT-01 Awareness and Training<br>Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind                                                                 | 2       | 3       | 3      |
| PR.DS-01 Data Security<br>The confidentiality, integrity, and availability of data-at-rest are protected                                                                                                                                                      | 1       | 3       | 3      |
| PR.DS-11 Data Security<br>Backups of data are created, protected, maintained, and tested                                                                                                                                                                      | 2       | 3       | 3      |
| PR.PS-02 Platform Security<br>Software is maintained, replaced, and removed commensurate with risk                                                                                                                                                            | 2       | 3       | 3      |

| Subcategory                                                                                                                                              | Earlier | Current | Target |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|--------|
| DE.CM-09 Continuous Monitoring<br>Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events | 2       | 3       | 3      |
| RC.RP-03 Incident Recovery Plan Execution<br>The integrity of backups and other restoration assets is verified before using them for restoration         | 1       | 3       | 3      |

## GAPS STILL OPEN, LARGEST FIRST

| Subcategory                                                                                                                                                                             | Current | Target | Gap | Linked risk |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------|-----|-------------|
| PR.PS-04 Platform Security<br>Log records are generated and made available for continuous monitoring                                                                                    | 1       | 3      | 2   | Very High   |
| PR.IR-01 Technology Infrastructure Resilience<br>Networks and environments are protected from unauthorized logical access and usage                                                     | 1       | 3      | 2   | Very High   |
| RC.RP-01 Incident Recovery Plan Execution<br>The recovery portion of the incident response plan is executed once initiated from the incident response process                           | 1       | 3      | 2   | Very High   |
| GV.SC-06 Cybersecurity Supply Chain Risk Management<br>Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships | 1       | 3      | 2   | High        |
| DE.CM-03 Continuous Monitoring<br>Personnel activity and technology usage are monitored to find potentially adverse events                                                              | 1       | 3      | 2   | High        |
| RS.MA-01 Incident Management<br>The incident response plan is executed in coordination with relevant third parties once an incident is declared                                         | 1       | 3      | 2   | Moderate    |
| RS.CO-02 Incident Response Reporting and Communication<br>Internal and external stakeholders are notified of incidents                                                                  | 1       | 3      | 2   | Moderate    |
| GV.OC-04 Organizational Context<br>Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated | 1       | 3      | 2   | -           |
| GV.RM-01 Risk Management Strategy<br>Risk management objectives are established and agreed to by organizational stakeholders                                                            | 1       | 3      | 2   | -           |
| GV.RM-02 Risk Management Strategy<br>Risk appetite and risk tolerance statements are established, communicated, and maintained                                                          | 0       | 2      | 2   | -           |
| GV.RM-05 Risk Management Strategy<br>Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties     | 1       | 3      | 2   | -           |
| GV.RR-03 Roles, Responsibilities, and Authorities<br>Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies          | 1       | 3      | 2   | -           |
| GV.OV-01 Oversight<br>Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction                                                          | 1       | 3      | 2   | -           |

| Subcategory                                                                                                                                                                                                             | Current | Target | Gap | Linked risk |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------|-----|-------------|
| GV.OV-03 Oversight<br>Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed                                                                                         | 0       | 2      | 2   | -           |
| GV.SC-01 Cybersecurity Supply Chain Risk Management<br>A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders | 1       | 3      | 2   | -           |
| GV.SC-08 Cybersecurity Supply Chain Risk Management<br>Relevant suppliers and other third parties are included in incident planning, response, and recovery activities                                                  | 1       | 3      | 2   | -           |
| ID.AM-03 Asset Management<br>Representations of the organization's authorized network communication and internal and external network data flows are maintained                                                         | 1       | 3      | 2   | -           |
| ID.AM-05 Asset Management<br>Assets are prioritized based on classification, criticality, resources, and impact on the mission                                                                                          | 1       | 3      | 2   | -           |
| ID.AM-07 Asset Management<br>Inventories of data and corresponding metadata for designated data types are maintained                                                                                                    | 1       | 3      | 2   | -           |
| ID.RA-06 Risk Assessment<br>Risk responses are chosen, prioritized, planned, tracked, and communicated                                                                                                                  | 1       | 3      | 2   | -           |
| ID.RA-08 Risk Assessment<br>Processes for receiving, analyzing, and responding to vulnerability disclosures are established                                                                                             | 0       | 2      | 2   | -           |
| ID.IM-01 Improvement<br>Improvements are identified from evaluations                                                                                                                                                    | 1       | 3      | 2   | -           |
| ID.IM-02 Improvement<br>Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties                                                   | 0       | 2      | 2   | -           |
| ID.IM-04 Improvement<br>Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved                                                            | 1       | 3      | 2   | -           |
| PR.AT-02 Awareness and Training<br>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   | 1       | 3      | 2   | -           |

And 67 more smaller gaps, listed in the current assessment report.

Linked risk: the highest-rated risk in the current assessment that names the subcategory.

## RISKS

2 risks closed, 1 new, 3 re-rated and 4 still open with the same rating. Risks are matched by ID, then by title; a risk that is not in the current assessment is counted as closed.

## CLOSED

| Risk                                   | Rated then |
|----------------------------------------|------------|
| R-09 Backups fail when they are needed | High       |
| R-10 Staff fall for phishing           | Moderate   |

## NEW

| Risk                                 | Rated now | Owner       |
|--------------------------------------|-----------|-------------|
| R-08 Unpatched firewall is exploited | Moderate  | IT provider |

## RE-RATED

| Risk                                             | Then     | Now             | Score             |
|--------------------------------------------------|----------|-----------------|-------------------|
| R-02 Business email compromise diverts a payment | Moderate | <b>High</b>     | 12 -> 16 (higher) |
| R-05 Lost or stolen device exposes patient data  | Moderate | <b>Moderate</b> | 12 -> 9 (lower)   |
| R-06 Departing staff keep access                 | Moderate | <b>Low</b>      | 12 -> 8 (lower)   |

Score: likelihood times impact, each from 1 (very low) to 5 (very high).

## STILL OPEN, SAME RATING

| Risk                                                     | Rated     |
|----------------------------------------------------------|-----------|
| R-01 Ransomware stops patient care and exposes records   | Very High |
| R-03 IT provider compromise reaches the practice         | High      |
| R-04 Breach is not reported on time                      | Moderate  |
| R-07 Long outage at the cloud practice-management vendor | Low       |