

Sample Dental Group (made up)

ACTION REQUIRED

Q3 2026 · Jul 1, 2026 to Sep 30, 2026

Two risks were closed and the first vulnerability scans are done, but the practice is not yet where it needs to be: replacing the out-of-support X-ray PC is past due, and staff email sign-in is still the biggest exposure.

7**OPEN RISKS**

Down 2 since Q2 2026

3**ABOVE APPETITE**

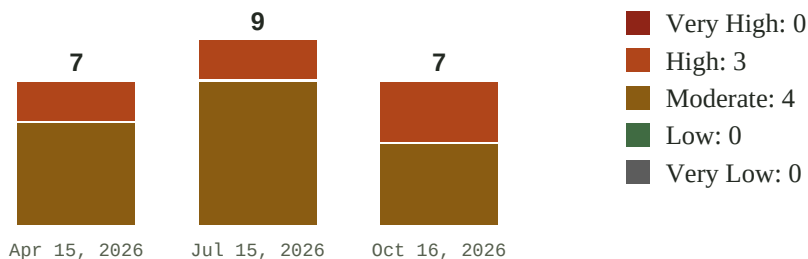
Up 1 since Q2 2026

1**PAST DUE**

Up 1 since Q2 2026

2**CLOSED THIS PERIOD****3****NEW THIS PERIOD**

OPEN RISKS OVER TIME



TOP RISKS

Risk	Level	Owner	Due	Status
Panoramic X-ray PC runs Windows 10 with no security updates	High	Dr. R. Example, Owner	Sep 30, 2026 (past due)	Open
Phishing leads to a staff Microsoft 365 mailbox takeover	High	Chris Example, ExampleTech	Oct 31, 2026	In treatment
Ransomware encrypts the patient chart and imaging servers	High	Chris Example, ExampleTech	Dec 15, 2026	Open
One person can change where payments are sent	Moderate	Dana Sample, Office Manager	Oct 31, 2026	In treatment
Software vendor signs in with a shared, always-on account	Moderate	Dana Sample, Office Manager	Nov 30, 2026	Open

The business has agreed to carry risks up to Moderate. Anything higher needs a funded plan or a recorded acceptance.

DECISIONS OR SUPPORT NEEDED FROM THE BOARD

- Approve the \$4,800 replacement of the panoramic X-ray PC this month. The fix is past due and the PC is the most exposed system in the practice.
- Approve the off-site backup service, about \$150 a month, so a ransomware attack cannot take the backups too.
- Confirm that every mailbox, including both doctors', will require a second sign-in step by Oct 31.

WHAT WAS DONE THIS PERIOD

- Closed: both doctors' laptops are encrypted (Aug 20).
- Closed: a leaver checklist is in use and two old staff accounts were removed (Sep 12).
- First external and internal vulnerability scans (Sep 8 and 9): 6 findings, 1 fixed and 1 awaiting retest.
- Payments: a call-back rule for bank changes and a second approver over \$2,500, in effect from Oct 1.
- Phishing and payment-fraud refresher: 13 of 14 staff completed it.

PROGRAM MATURITY

NIST CSF 2.0 average: 1.8 of 5, against a target of 3.1.



Bar: where the practice is today. Marker: the agreed target.

MEASURES

Measure		Q1 2026	Q2 2026	Q3 2026	Target	Status
Days to fix critical and high findings (average)	KPI	-	-	11 days	30 days	On target
Staff who completed security training	KPI	86%	86%	92.9%	95%	Off target, improving
Tier 1 vendors with a current review	KPI	33%	50%	66.7%	100%	Off target, improving
Critical patches applied within 14 days	KPI	70%	82%	88%	95%	Off target, improving
Privileged accounts without MFA	KRI	3	2	1	0	Off target, improving
Risks above the agreed appetite	KRI	-	2	3	0	Off target, worse
Risk treatments past due	KRI	-	0	1	0	Off target, worse
Test findings past the fix-by date	KRI	-	-	2	0	Off target
Staff who clicked in the last phishing test	KRI	-	21.4%	7.1%	5%	Off target, improving
Critical or high assets with no owner	KRI	-	-	1	0	Off target
Security incidents this period	KRI	0	1	0	0	On target, improving

KPI: how well the program is performing. KRI: how exposed the business is.

INCIDENTS AND NEAR MISSES

None in the quarter. After it closed, on Oct 13, the office manager's mailbox was taken over through a fake sign-in page and one vendor payment of \$18,400 was sent to a fraudulent account; the bank recall is in progress. It will be

covered in full in the Q4 report, and it is why multi-factor sign-in is the first priority below.

PRIORITIES FOR NEXT PERIOD

- Second sign-in step on all 14 mailboxes by Oct 31.
- Replace the panoramic X-ray PC, and keep it on its own network until then.
- Off-site, immutable backups and a timed restore of both servers.
- Named support accounts with MFA for ExampleChart.
- Write the incident response plan and run a one-hour tabletop in January.

SECURITY TESTING

5 of 6 security test findings are still open; 3 are rated critical or high, and 2 are past the fix-by date.

STAFF AWARENESS

13 of 14 staff (93%) completed "Phishing and payment fraud refresher" (Aug 28, 2026), compared with 86% in the round before. 7.1% of staff clicked in the last phishing test (Sep 17, 2026), and 50% reported it. The test before was 21.4%.

Date	Type	Name	Result
Mar 20, 2026	Training	Annual HIPAA and security awareness	86% completed (12 of 14)
May 14, 2026	Phishing test	Shared invoice lure	21.4% clicked
Aug 28, 2026	Training	Phishing and payment fraud refresher	93% completed (13 of 14)
Sep 17, 2026	Phishing test	Package delivery lure	7.1% clicked

ACCEPTED RISKS

1 risk has been accepted. Details and sign-off are in the risk register.