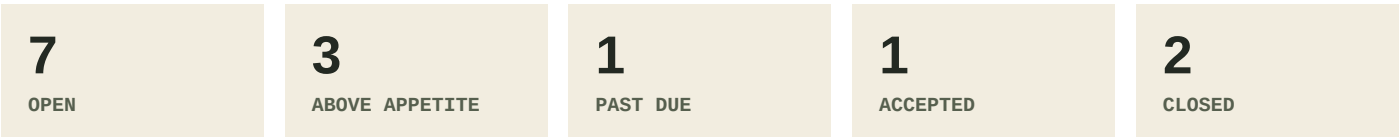


EXAMPLE SECURITY PARTNERS

RISK REGISTER

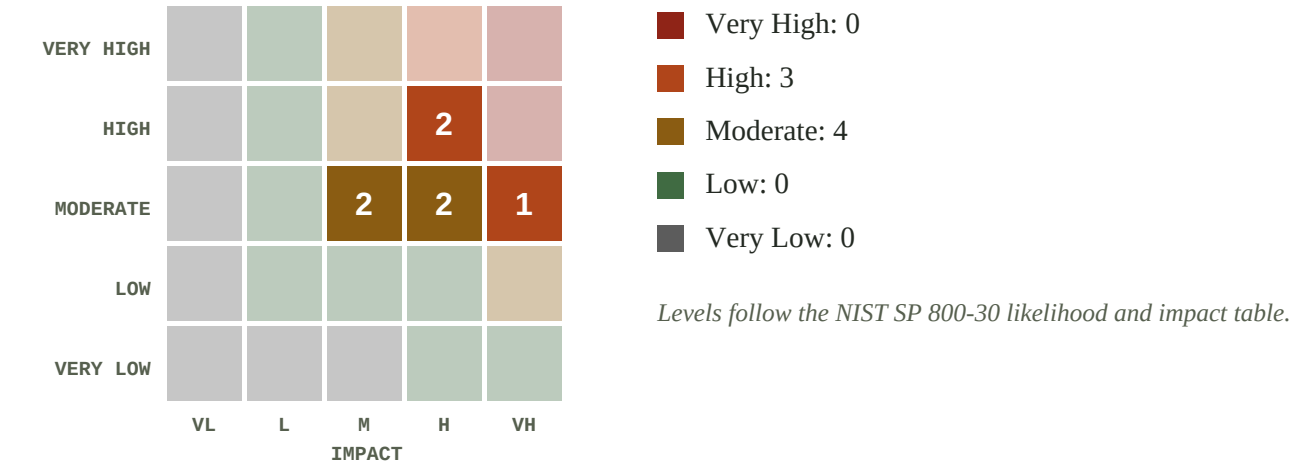
Sample Dental Group (made up)

As of Oct 16, 2026 · Register owner: Dana Sample, Office Manager · Risk appetite: Moderate · Next review: Jan 15, 2027



OPEN RISKS BY LIKELIHOOD AND IMPACT

LIKELIHOOD



OPEN RISKS

ID	Risk	Level	Response	Owner	Due	Status
R-03	Panoramic X-ray PC runs Windows 10 with no security updates	High	Mitigate	Dr. R. Example, Owner	Sep 30, 2026 (past due)	Open
R-01	Phishing leads to a staff Microsoft 365 mailbox takeover	High	Mitigate	Chris Example, ExampleTech	Oct 31, 2026	In treatment
R-02	Ransomware encrypts the patient chart and imaging servers	High	Mitigate	Chris Example, ExampleTech	Dec 15, 2026	Open
R-05	One person can change where payments are sent	Moderate	Mitigate	Dana Sample, Office Manager	Oct 31, 2026	In treatment
R-04	Software vendor signs in with a shared, always-on account	Moderate	Mitigate	Dana Sample, Office Manager	Nov 30, 2026	Open
R-07	Booking website runs out-of-date plugins	Moderate	Mitigate	Dana Sample, Office Manager	Dec 31, 2026	Open
R-06	No written, tested incident response plan	Moderate	Mitigate	Dana Sample, Office Manager	Jan 31, 2027	Open

RISKS ABOVE APPETITE

R-03 Panoramic X-ray PC runs Windows 10 with no security updates

HIGH

WHAT COULD HAPPEN

A known Windows flaw is used to take over the X-ray acquisition PC and move to the imaging server.

WHY IT IS POSSIBLE TODAY

SDG-PANO still runs Windows 10, which stopped receiving security updates in October 2025, and the imaging vendor has always-on remote access to it.

WHAT IT WOULD COST THE BUSINESS

Loss of panoramic imaging and a foothold on the clinical network. Estimated loss: \$8,000 to \$40,000.

TREATMENT PLAN

Replace the PC with a Windows 11 unit the imaging vendor supports; until then, isolate it on its own network segment. The replacement was quoted at \$4,800 and is waiting on the owner's approval; the vendor needs two weeks to install and calibrate it.

OWNER AND DATE

Dr. R. Example, Owner · Sep 30, 2026 · Expected level after treatment: Low

R-01 Phishing leads to a staff Microsoft 365 mailbox takeover

HIGH

WHAT COULD HAPPEN

An attacker steals a staff password with a fake sign-in page, reads patient emails and sends fake invoices from a trusted mailbox.

WHY IT IS POSSIBLE TODAY

Only 5 of 14 mailboxes require a second sign-in step, and nobody reviews sign-in alerts.

WHAT IT WOULD COST THE BUSINESS

A reportable HIPAA breach, fraudulent payments and several days of disruption at the front desk. Estimated loss: \$15,000 to \$120,000.

TREATMENT PLAN

Require multi-factor authentication on all 14 mailboxes, block legacy sign-in, and send sign-in alerts to ExampleTech's help desk.

OWNER AND DATE

Chris Example, ExampleTech · Oct 31, 2026 · Expected level after treatment: Low

R-02 Ransomware encrypts the patient chart and imaging servers

HIGH

WHAT COULD HAPPEN

Ransomware spreads from one workstation to SDG-PMS01 and SDG-IMG01 and encrypts patient charts and X-rays.

WHY IT IS POSSIBLE TODAY

Nightly backups go to SDG-NAS01 on the same network with the same admin account, and a full restore has never been tested.

WHAT IT WOULD COST THE BUSINESS

The practice cannot see patients' charts or images; about four days of cancelled appointments plus breach notification. Estimated loss: \$60,000 to \$250,000.

TREATMENT PLAN

Add an immutable off-site copy with Example Cloud Backup, separate the backup admin account, and run a timed restore of both servers each quarter. Budget approved at the July review; ExampleTech is setting it up in November.

OWNER AND DATE

Chris Example, ExampleTech · Dec 15, 2026 · Expected level after treatment: Low

ACCEPTED RISKS

ID	Risk	Level	Accepted by	On	Revisit by
R-08	Imaging software needs local admin rights on operatory PCs	Moderate	Dr. R. Example, Owner	Aug 5, 2026	Feb 5, 2027

By signing, the client confirms it understands the accepted risks listed above and chooses to carry them until the revisit date.

NAME, ROLE AND SIGNATURE

DATE

CLOSED RISKS

ID	Risk	Closed	Notes
R-09	Lost or stolen doctor laptop exposes patient records	Aug 20, 2026	BitLocker confirmed on both laptops.
R-10	Former staff keep access to email and the practice-management system	Sep 12, 2026	Leaver checklist in use since July.

SECURITY TESTING

ID	Type	Tester	Dates	Findings	Open	Next test
T-01	Vulnerability scan	ExampleTech Managed IT	Sep 8, 2026 to Sep 9, 2026	6	5	Dec 8, 2026

ID	Open finding	Severity	System	Owner	Fix by	Status
F-02	Windows 10 out of support	Critical	SDG-PANO	Dr. R. Example	Sep 24, 2026 (past due)	Open
F-01	Firewall admin page open to internet	High	SDG-FW01 (203.0.113.10)	ExampleTech	Oct 8, 2026 (past due)	In progress
F-03	SMBv1 file sharing enabled	High	SDG-NAS01	ExampleTech	Oct 9, 2026	Fixed, awaiting retest
F-05	Missing Windows updates	Medium	SDG-OP2	ExampleTech	Dec 8, 2026	In progress
F-06	Website allows TLS 1.0	Medium	booking.sample-dental.example	Dana Sample	Dec 7, 2026	Open

REVIEW HISTORY

Date	Reviewed with	Open	VH	H	M	Past due	Closed since last	Note
Oct 16, 2026	Dr. R. Example, Dana Sample	7	0	3	4	1	2	Scan findings added; X-ray PC replacement late.
Jul 15, 2026	Dr. R. Example, Dana Sample	9	0	2	7	0	0	Laptop encryption under way; payment fraud risk added.
Apr 15, 2026	Dr. R. Example, Dana Sample	7	0	2	5	0	0	First review after the assessment.