

EXAMPLE SECURITY PARTNERS

BOARD BRIEFING

Cybersecurity Risk Assessment

NIST Cybersecurity Framework 2.0 · Current and target profile

Sample Dental Group (made up)

October 16, 2026 · Presented by Alex Sample, CISSP

THE BOTTOM LINE

3 high or very high risks need board attention

1.5

AVG MATURITY TODAY (0-5)

2.6

TARGET MATURITY

T1 → 2

CSF TIER, CURRENT → TARGET

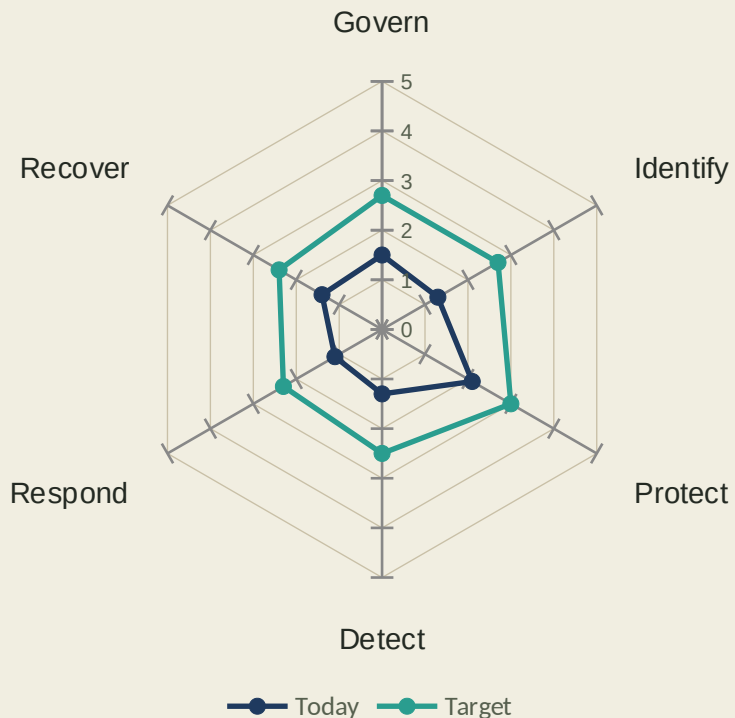
3

HIGH / VERY HIGH RISKS

The practice has good habits in the places HIPAA has pushed it: a signed security policy, encrypted devices, monthly patching, managed endpoint protection and tested backups. The gaps are in what holds those habits together: there is no tested plan for an incident or a restore, the network is flat, MFA is incomplete, and nobody reviews the logs or the IT provider's access.

WHERE WE STAND

Today vs. where we need to be

**LARGEST GAPS****Identify**

1.3 today → 2.7 target

Respond

1.1 today → 2.3 target

Govern

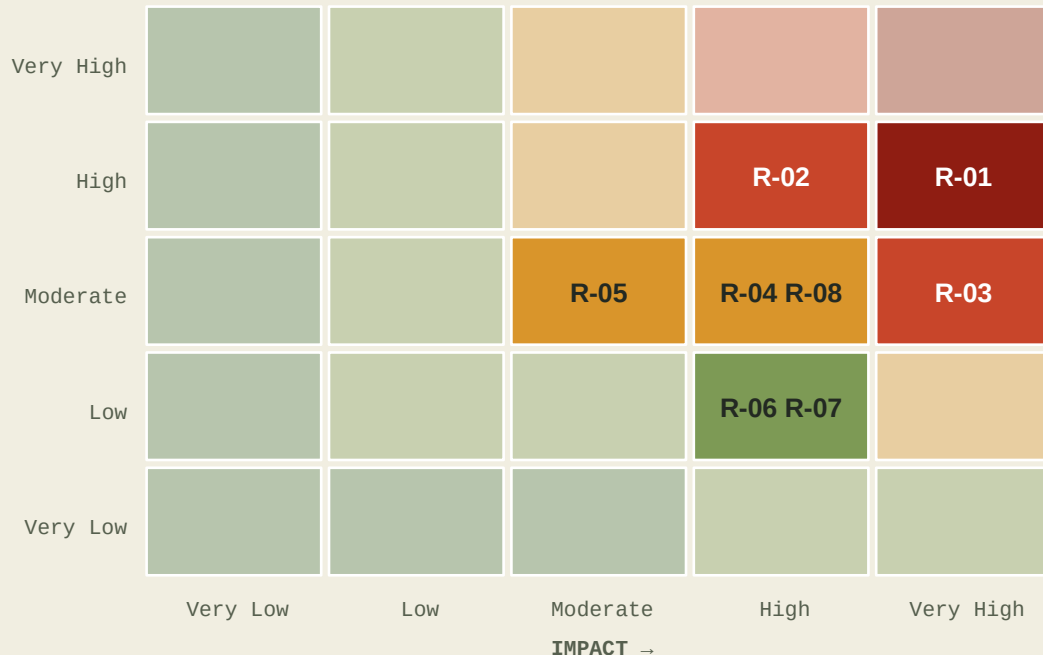
1.5 today → 2.7 target

STRENGTH Tested offsite backups, full device encryption, endpoint protection on every device, and 100% staff training.

RISK PICTURE

8 risks assessed · likelihood × impact

LIKELIHOOD



1 Very high

2 High

3 Moderate

2 Low

0 Very low

TOP RISKS

The risks that matter most

R-01

Ransomware stops patient care and exposes records

Put MFA on every remote path, separate imaging and staff networks, and write and test a recovery plan.

VERY HIGH

Mitigate

R-02

Business email compromise diverts a payment

Enforce MFA on all mailboxes, turn on risky sign-in alerts, and require a call-back and two approvers for bank changes.

HIGH

Mitigate

R-03

IT provider compromise reaches the practice

Require MFA and session logging on the remote tool, and add security and notice terms at the contract renewal.

HIGH

Mitigate

R-04

Breach is not reported on time

Approve the incident response plan with a notice checklist and the insurer's breach line, and rehearse it once a year.

MODERATE

Mitigate

R-05

Lost or stolen device exposes patient data

Enroll staff phones that get email in device management, with remote wipe.

MODERATE

Mitigate

THE ROADMAP

Highest risks first, over 12 months

0–90 DAYS

3 actions

- R-01 Put MFA on every remote path, separate imaging and staff...
- R-02 Enforce MFA on all mailboxes, turn on risky sign-in alerts,...
- R-03 Require MFA and session logging on the remote tool, and add...

3–6 MONTHS

3 actions

- R-04 Approve the incident response plan with a notice checklist...
- R-05 Enroll staff phones that get email in device management,...
- R-08 Update the firewall now and add quarterly external...

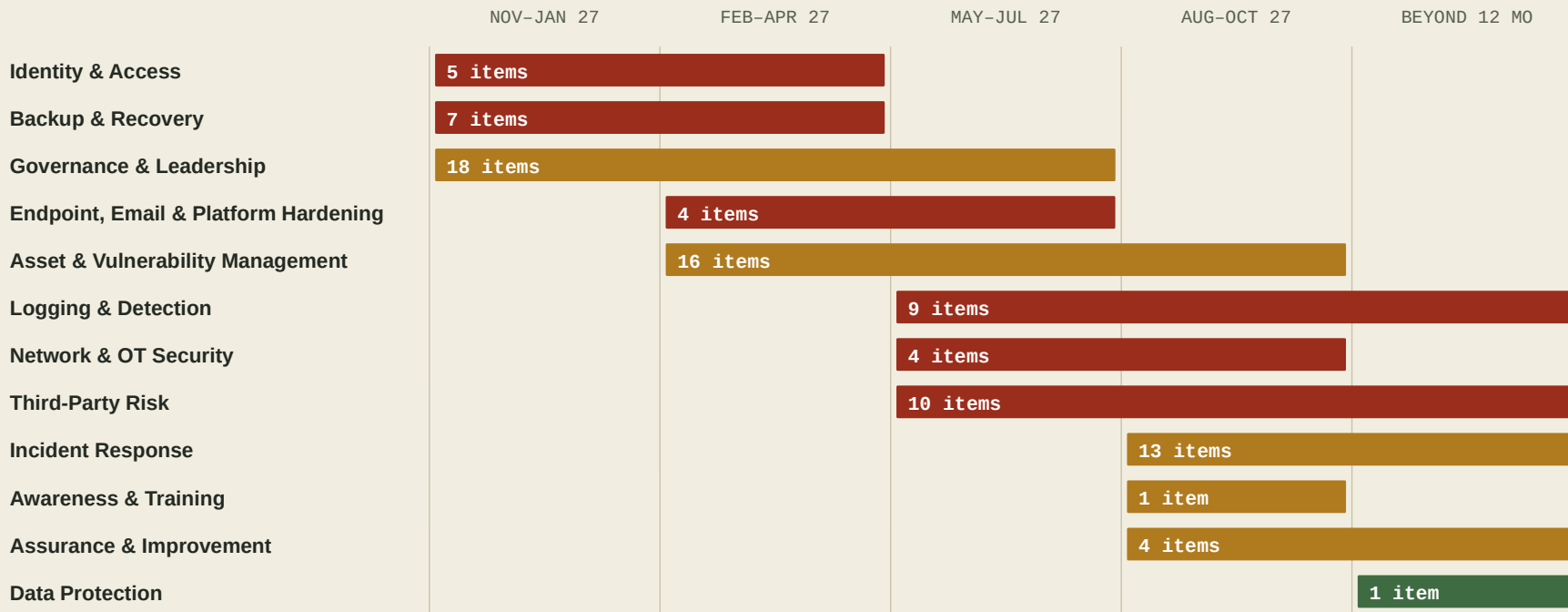
6–12 MONTHS

1 action

- R-06 Replace shared logins and review PMS and email access each...

INITIATIVE TIMELINE

Twelve months, sequenced by priority



DECISIONS REQUESTED

What we need from the board

1

Approve the risk roadmap

Endorse the plan and owners for 7 risk treatments.

2

Formally accept residual risk

1 risk (R-07) recommended for acceptance need board sign-off.

3

Set the target

Adopt CSF Tier 2 and an average maturity of 2.6 as the goal.

4

Oversee progress

Quarterly risk updates to the board; reassess annually.

ASSESSOR'S RECOMMENDATION

Approve a security budget of about \$14,000 for the next 12 months (network separation, log collection and an annual outside test), and ask the IT provider to accept security terms at its contract renewal.

Questions

Alex Sample, CISSP

vCISO · Security Consultant · Incident Response Advisor

hello@example.com · example.com

The full assessment report contains detailed findings, evidence, and methodology.