

CYBER INSURANCE READINESS

Sample Dental Group (made up) · Renewal or application Dec 1, 2026 · Prepared Oct 16, 2026

13

PROVEN IN PLACE

2

YES, NOT PROVEN

6

PARTLY

3

NO OR NOT SURE

6/9

CRITICAL PROVEN

Insurers increasingly ask for proof alongside the application, scan the business from outside, and can deny a claim when an answer turns out to be wrong. So this report counts a control as in place only when it is answered Yes, covers everything it should, and has evidence dated within 90 days of the application.

3 of the 9 critical controls are not yet proven in place. They come first in the plan below.

FIX OR PROVE BEFORE APPLYING

Priority	Control	What to do	Owner	Fix by
Critical Partly	Is MFA required for all remote access to the network (VPN, remote desktop, remote management tools)?	Put every remote path behind MFA; remove remote tools nobody needs, including the IT provider's spares.	IT provider	Nov 6, 2026
Critical Partly	Is remote desktop (RDP) or any other remote-access service closed to the open internet?	Close inbound RDP and admin ports at the firewall; reach them only through a VPN with MFA.	IT provider	Oct 31, 2026
Critical Partly	Must payment and bank-detail change requests be verified by phone using a known number before money is sent?	Write a call-back rule for any new payee or changed bank details, using a number already on file, and train finance staff on it.	Practice administrator	Oct 31, 2026
Important No	Are systems scanned for vulnerabilities at least once a year?	Run an internal and external scan and fix findings in priority order; repeat at least yearly.	IT provider	Nov 20, 2026
Important No	Are security logs collected and monitored, by staff, the IT provider or a managed detection service?	Send security logs to a monitored service and keep them at least 90 days.	IT provider	Feb 26, 2027
Important Partly	Is incoming email filtered for malicious links and attachments, with SPF, DKIM and DMARC set up for the domain?	Turn on advanced filtering and publish SPF, DKIM and a DMARC policy, moving to quarantine or reject.	IT provider	Nov 30, 2026
Important Partly	Does the business have a written incident response plan?	Write a short plan: who to call, how to isolate systems, the insurer's hotline, and who may speak publicly.	Practice administrator	Nov 13, 2026
Important Yes, not proven	Are all operating systems and key software still supported by the vendor?	Collect: Asset list with operating-system versions.	IT provider	Oct 30, 2026
Standard No	Has the incident response plan been tested, for example with a tabletop exercise, in the last 12 months?	Run a 90-minute tabletop exercise and fix what it shows.	Managing dentist	Nov 20, 2026

Priority	Control	What to do	Owner	Fix by
Standard Partly	Are vendors with access to systems or sensitive data reviewed for security?	List vendors with access, review the important ones yearly, and add security terms to contracts.	Practice administrator	Nov 30, 2026
Standard Yes, evidence out of date	Is there an up-to-date list of the business's computers, servers and cloud services?	Collect again (older than 90 days): Asset inventory with last-updated date.	IT provider	Nov 6, 2026

WHAT INSURERS SEE FROM OUTSIDE

Check	Result	Date
X-01 Email domain records (sampledental.example.com)	SPF v=spf1 include:spf.protection.outlook.com -all; DMARC v=DMARC1; p=none; rua=mailto:dmarc@sampledental.example.com	Oct 2, 2026
X-02 Remote desktop or admin ports open to the internet	Found: Firewall admin page on 203.0.113.18 (port 8443); no remote desktop	Oct 2, 2026
X-03 Expired or invalid certificates on public websites or VPN	None found	Oct 2, 2026
X-04 Staff accounts on the client's domain found in known breaches	Found: 3 staff addresses in older public breaches; passwords since changed	Oct 2, 2026

THE QUESTION MAP

Access

Question	Status	Proof	Notes
Is multi-factor authentication (MFA) required for all email access, including webmail and phones? [Critical]	Yes	2 of 2 items collected. 14 of 14 mailboxes with MFA enforced. E-01 MFA or conditional-access report from the email admin console (Oct 14, 2026, IT provider or MSP); E-02 User list showing MFA registered for every mailbox (Oct 14, 2026, IT provider or MSP)	Enforced for the last 3 mailboxes on Oct 14 during the email-fraud response.
Is MFA required for all remote access to the network (VPN, remote desktop, remote management tools)? [Critical]	Partly	1 of 2 items collected. 1 of 2 remote-access paths behind MFA. E-03 VPN or remote-access settings showing MFA required (Oct 6, 2026, IT provider or MSP)	VPN requires MFA; the IT provider's remote-support tool does not.
Is MFA required for all administrator and privileged accounts, including cloud, backup and email admin? [Critical]	Yes	1 of 1 items collected. 4 of 4 admin accounts with MFA. E-05 Admin account list with MFA status, including IT provider and break-glass accounts (Oct 6, 2026, IT provider or MSP)	
Is remote desktop (RDP) or any other remote-access service closed to the open internet? [Critical]	Partly	2 of 2 items collected. E-06 External scan showing no remote desktop or admin ports open (Oct 2, 2026, Our review); E-07 Firewall rule review (Oct 2, 2026, Our review)	Remote desktop is closed; the firewall admin page is open to the internet.
Do staff use separate accounts for administrator work, with everyday accounts lacking admin rights?	Yes	1 of 1 items collected. E-08 List of admin accounts and who holds them (Oct 6, 2026, IT provider or MSP)	

Question	Status	Proof	Notes
Is access removed promptly when someone leaves the business?	Yes	1 of 1 items collected. E-09 Leaver checklist and one recent completed example (Sep 15, 2026, Client)	

Devices and patching

Question	Status	Proof	Notes
Is endpoint detection and response (EDR) or next-generation antivirus installed on every computer and server? [Critical]	Yes	2 of 2 items collected. 22 of 22 computers and servers with EDR. E-10 EDR console export listing every protected device (Oct 2, 2026, IT provider or MSP); E-11 RMM or asset list to compare it against (Oct 2, 2026, IT provider or MSP)	
Are critical security updates applied within 30 days, or sooner when actively exploited?	Yes	1 of 2 items collected. E-12 RMM or update-tool patch compliance report (Oct 5, 2026, IT provider or MSP)	
Are all operating systems and key software still supported by the vendor?	Yes, not proven	0 of 1 items collected	
Are systems scanned for vulnerabilities at least once a year?	No	0 of 2 items collected	

Backups

Question	Status	Proof	Notes
Are critical data and systems backed up at least weekly? [Critical]	Yes	1 of 1 items collected. 3 of 3 critical systems backed up. E-17 Backup job report listing systems, frequency and success (Sep 30, 2026, IT provider or MSP)	Imaging server, Microsoft 365 mailboxes and files, and the scanned-forms share.
Is at least one backup copy offline, immutable or otherwise separated so ransomware cannot reach it? [Critical]	Yes	1 of 1 items collected. E-18 Backup settings showing an offline or immutable copy with separate credentials (Sep 30, 2026, IT provider or MSP)	
Has a restore from backup been tested successfully in the last 12 months? [Critical]	Yes	1 of 1 items collected. E-19 Dated restore test record: what was restored and how long it took (Oct 7, 2026, Our review)	Imaging server restore witnessed Oct 7: 2 hours 40 minutes.

Email and staff

Question	Status	Proof	Notes
Is incoming email filtered for malicious links and attachments, with SPF, DKIM and DMARC set up for the domain?	Partly	2 of 2 items collected. E-20 Email filtering settings (Oct 6, 2026, IT provider or MSP); E-21 SPF, DKIM and DMARC records, or a DMARC report (Oct 2, 2026, Our review)	Filtering on; DMARC is p=none.
Do all staff complete security awareness training at least once a year?	Yes	1 of 1 items collected. E-22 Training completion report with dates (Sep 10, 2026, Client)	

Question	Status	Proof	Notes
Are phishing simulations run with staff?	Yes	1 of 1 items collected. E-23 Phishing test results with dates (Sep 18, 2026, Client)	
Must payment and bank-detail change requests be verified by phone using a known number before money is sent? [Critical]	Partly	0 of 2 items collected	Call-back rule adopted Oct 14 after the email fraud; not yet written or signed by staff.

Response and governance

Question	Status	Proof	Notes
Does the business have a written incident response plan?	Partly	0 of 1 items collected	Draft from September; not yet approved.
Has the incident response plan been tested, for example with a tabletop exercise, in the last 12 months?	No	0 of 1 items collected	
Are security logs collected and monitored, by staff, the IT provider or a managed detection service?	No	0 of 1 items collected	
Is there an up-to-date list of the business's computers, servers and cloud services?	Yes, evidence out of date	1 of 1 items collected. E-29 Asset inventory with last-updated date (Nov 20, 2025, IT provider or MSP)	
Are vendors with access to systems or sensitive data reviewed for security?	Partly	1 of 1 items collected. E-30 Vendor list with review dates (Sep 24, 2026, Client)	Business associate agreements on file; no security review of vendors.
Are laptops and sensitive data encrypted?	Yes	1 of 1 items collected. 6 of 6 laptops encrypted. E-31 Device encryption report (BitLocker or FileVault) (Oct 1, 2026, IT provider or MSP)	
Are written security policies in place and approved by management?	Yes	1 of 1 items collected. E-32 Approved policies with approval dates (Sep 24, 2026, Client)	

Disclosure

Question	Status	Proof	Notes
In the last three to five years, have there been any cyber incidents, claims, or circumstances that could lead to a claim?	Yes		Email fraud on Oct 13, 2026: one \$18,400 vendor payment diverted; reported to the insurer and IC3 the same day; recall in progress.

Application wording differs between insurers. Answer each insurer's question as written, using this map as the record of what is true and what proves it. Evidence shows a control on the date it was collected; controls can change afterwards. This report does not promise coverage, terms or a price; the insurer decides.