

EXAMPLE SECURITY PARTNERS

VENDOR RISK REVIEW

Sample Dental Group (made up)

As of Oct 16, 2026 · Owner: Dana Sample, Office Manager

10 VENDORS	6 TIER 1	3 REVIEWS DUE	2 HIGH RISK	3 TERMS MISSING
---------------	-------------	------------------	----------------	--------------------

Tier 1 vendors hold regulated data, have administrator or remote access, or would stop operations if they failed; they get a full review every year. Tier 2 vendors get a short review every two years. Tier 3 vendors stay on the list without a review. Vendor risk combines the tier with how the vendor answered.

VENDOR LIST

Vendor	Service	Tier	Risk	Status	Owner	Next review
Example Claims Clearinghouse	Insurance claims and eligibility checks	Tier 1	High	Not reviewed	Dana Sample	Due now
Example Imaging Systems	Imaging software, X-ray sensors and panoramic unit support	Tier 1	High	In review	Dana Sample	Due now
Example Cloud Backup	Off-site, immutable copy of server backups	Tier 1	Low	Approved	Dana Sample	Sep 30, 2027
Example Payroll Services	Payroll, staff tax filings and direct deposit	Tier 1	Low	Approved	Dana Sample	Mar 10, 2027
ExampleChart Dental Software	Practice-management software and remote support	Tier 1	Low	Approved with conditions	Dana Sample	Sep 25, 2027
ExampleTech Managed IT	IT support, monitoring, patching and backups	Tier 1	Low	Approved	Dana Sample	Aug 15, 2027
Example Phone Co.	Phones, voicemail and call recording	Tier 2	Moderate	Not reviewed	Dana Sample	Due now
Example Dental Lab	Crowns and appliances; receives patient scans	Tier 2	Low	Approved	Dana Sample	Nov 4, 2027
Example Shredding	On-site shredding of paper records	Tier 2	Low	Approved	Dana Sample	Feb 12, 2028
Example Office Supply	Office and clinical supplies	Tier 3		Approved	Dana Sample	None

FINDINGS BY VENDOR

Example Claims Clearinghouse

HIGH RISK

Tier 1 · Insurance claims and eligibility checks · Data: Regulated data (health, payment card, government ID) · Access: Integration or data feed · If down for a week: Hard to operate for a week

Not yet assessed: fewer than half the questions are answered.

CONTRACT TERMS NOT CONFIRMED

- Notice of a security incident affecting the client within 72 hours
- Notice of confirmed vulnerabilities in the product or service
- Protection of the client's data at least as strong as the client's own
- Multi-factor authentication for any remote access to the client's systems
- The client may ask for evidence of security, such as a certification or report
- Return or destruction of the client's data at termination, confirmed in writing

Example Imaging Systems**HIGH RISK**

Tier 1 · Imaging software, X-ray sensors and panoramic unit support · Data: Regulated data (health, payment card, government ID) · Access: Administrator or remote access · If down for a week: Hard to operate for a week

Answers rate this vendor Weak. Evidence received: Completed questionnaire.

ANSWERED NO

- Access to our data is limited to staff who need it and is removed when they leave.

ANSWERED PARTLY

- Staff who can reach our data or systems must use multi-factor authentication.
- They back up the service, test restores, and can recover within the time we need.
- Critical security updates are applied within 30 days.
- Staff are screened and given security training each year.

NOT KNOWN OR NOT ANSWERED

- They have had an independent security audit in the last 12 months (SOC 2 Type II, ISO 27001 or similar).
- They have a written incident response plan and have tested it in the last year.
- Subcontractors who can reach our data are named and held to the same terms.
- They carry cyber liability insurance.

CONTRACT TERMS NOT CONFIRMED

- Notice of confirmed vulnerabilities in the product or service
- Multi-factor authentication for any remote access to the client's systems
- The client may ask for evidence of security, such as a certification or report

CONDITIONS OR FOLLOW-UP

- Confirm a supported operating system for the panoramic PC and a replacement date (risk R-03). Ask for an independent audit report.

Example Cloud Backup**LOW RISK**

Tier 1 · Off-site, immutable copy of server backups · Data: Regulated data (health, payment card, government ID) · Access: Integration or data feed · If down for a week: Hard to operate for a week

Answers rate this vendor Strong. Evidence received: SOC 2 Type II report, ISO 27001 certificate.

ANSWERED PARTLY

- They carry cyber liability insurance.

Example Payroll Services**LOW RISK**

Tier 1 · Payroll, staff tax filings and direct deposit · Data: Regulated data (health, payment card, government ID) · Access: Standard user accounts · If down for a week: Inconvenient for a few days

Answers rate this vendor Strong. Evidence received: SOC 2 Type II report, Cyber insurance certificate.

ExampleChart Dental Software

LOW RISK

Tier 1 · Practice-management software and remote support · Data: Regulated data (health, payment card, government ID) · Access: Administrator or remote access · If down for a week: Operations stop

Answers rate this vendor Strong. Evidence received: SOC 2 Type II report, Completed questionnaire.

ANSWERED PARTLY

- Staff who can reach our data or systems must use multi-factor authentication.
- Critical security updates are applied within 30 days.

CONTRACT TERMS NOT CONFIRMED

- Multi-factor authentication for any remote access to the client's systems

CONDITIONS OR FOLLOW-UP

- Replace the shared support account with named accounts that use MFA by Dec 31, 2026 (risk R-04).

ExampleTech Managed IT

LOW RISK

Tier 1 · IT support, monitoring, patching and backups · Data: Regulated data (health, payment card, government ID) · Access: Administrator or remote access · If down for a week: Operations stop

Answers rate this vendor Strong. Evidence received: Penetration test summary, Cyber insurance certificate, Completed questionnaire.

Example Phone Co.

MODERATE RISK

Tier 2 · Phones, voicemail and call recording · Data: Internal business information · Access: None · If down for a week: Hard to operate for a week

Not yet assessed: fewer than half the questions are answered.