SITE survey. APP

SITE SURVEY REPORT

IT Risk Assessment

Prepared for	Penrose Veterinary Group
Date	22 Sep 2026
Site	Penrose Veterinary Group, Exeter
Prepared by	S. Kowalczyk

FORM

IT Risk Assessment

1. Record details and scope

Project	Penrose Veterinary Group, Exeter: booking and records IT risk assessment
Client or organisation	Penrose Veterinary Group
Site or premises address	Penrose Veterinary Group, 18 Alder Lane, Exeter EX2
Record date	22 Sep 2026
Person completing the record	S. Kowalczyk

This is a risk decision record, not a vulnerability scan, penetration test, Cyber Essentials certificate or authorisation to test systems. Do not enter passwords or secret keys.

NCSC recommends choosing an approach that helps the organisation understand its actual cyber risks. Its framework considers context, decision makers, risk analysis, communication, implementation and review; no single method suits every situation. ISO/IEC 27005:2022 (guidance on information security risk management) is a recognised method you can name in section 2.

2. Scope and method

Business service and system boundary	Online appointment booking and client records, hosted by a third-party supplier, plus 4 reception PCs across two branches
Service owner and risk decision maker	Practice manager J. Tremayne, risk decisions by director A. Whitlock
Key information, suppliers and dependencies	Hosted practice management system from one supplier, branch broadband lines, hosted email and file storage, card payment terminals (out of scope)
Risk method, scale and acceptance policy	5 x 5 likelihood and impact scale from policy ISP-03 rev 2. Scores of 15 or more need director approval of the treatment.

3. Risk scenarios

Cyber risk 1: Phishing email leads to a stolen staff account and access to client records

Threat event and affected service	Phishing email leads to a stolen staff account and access to client records
Exposure, weakness and evidence	Multi-factor sign-in not switched on for 6 of 22 staff accounts. Click rate of 14% in the August phishing test.
Business consequences	Client personal data exposed, possible breach reporting, loss of trust, time lost resetting accounts

Existing controls and assurance evidence	Email filtering, annual awareness training, multi-factor sign-in on 16 accounts
Likelihood assessment and basis	4, based on test results and incidents reported in the sector
Risk priority using the stated method	16 (4 x 4), high
Treatment decision	Reduce
Treatment or acceptance rationale	Turn on multi-factor sign-in for all accounts and run phishing training each quarter.
Accountable risk owner	J. Tremayne, practice manager

Cyber risk 2: Malware on a reception PC stops bookings at a branch

Threat event and affected service	Malware on a reception PC stops bookings at a branch
Exposure, weakness and evidence	Two reception PCs run an operating system that no longer gets security updates
Business consequences	Branch cannot take bookings or view records for up to 2 days
Existing controls and assurance evidence	Endpoint protection, records held and backed up by the hosting supplier
Likelihood assessment and basis	3, unsupported systems but limited browsing on reception PCs
Risk priority using the stated method	12 (3 x 4), medium
Treatment decision	Reduce
Treatment or acceptance rationale	Replace both PCs by the end of November, budget approved.
Accountable risk owner	S. Kowalczyk, IT lead

Cyber risk 3: Supplier outage takes the online booking service offline

Threat event and affected service	Supplier outage takes the online booking service offline
Exposure, weakness and evidence	Single supplier, contracted availability 99.5%
Business consequences	Online bookings unavailable during the outage, more calls to reception
Existing controls and assurance evidence	Supplier status page, phone booking workaround in reception procedure
Likelihood assessment and basis	2, two short outages in the past year
Risk priority using the stated method	6 (2 x 3), low
Treatment decision	Accept
Treatment or acceptance rationale	Within the risk appetite in ISP-03. Keep the phone workaround and review at contract renewal.

Accountable risk owner	A. Whitlock, director
Risks recorded	3
Reduce	2
Accept	1
Pending decision	0

4. Assurance and review

How controls will be checked	Multi-factor sign-in report from the admin console checked monthly by the practice manager. PC replacement tracked on the IT plan. Supplier restore test evidence requested twice a year.
Next review date	22 Mar 2027
Days to the next review	182
Changes or incidents that trigger reassessment	A new branch, a new system or supplier, a data breach, or a major security incident at the supplier.
Authorised acceptance or treatment approval reference	Treatments and acceptance of risk 3 approved by director A. Whitlock, ref RA-APP-2026-09

5. Actions and review

Are further actions required?	Yes

Further action 1: Switch on multi-factor sign-in for the remaining 6 accounts.

Action and evidence reference	Switch on multi-factor sign-in for the remaining 6 accounts.
Person responsible	J. Tremayne, practice manager
Target date	15 Oct 2026
Action status	In progress

Further action 2: Replace the two unsupported reception PCs.

Action and evidence reference	Replace the two unsupported reception PCs.
Person responsible	S. Kowalczyk
Target date	30 Nov 2026
Action status	Open
Actions not completed	2

Outstanding limitations and information to pass on	Card payment terminals and the supplier's own controls were not assessed. Technical details kept out of this record.
Record status	Ready for review
Reviewed by	A. Whitlock
Review date	25 Sep 2026
Author signature	

Signing records the information entered. It does not itself certify legal compliance, remove a limitation or authorise unsafe work.