

SAMPLE PAGE · NAMES AND FIGURES GENERALISED

Imaging Practice IT Risk Audit

This is a representative sample of the 12 page Audit deliverable. Practice name, dates, financial figures, and specific identifiers have been generalised. Findings are realistic across multiple Australian imaging practices we have audited; your Audit will reflect your specific environment, evidence, and revenue.

Executive summary excerpt

Field	Value
Practice	[Imaging Group, 4 sites, ~78 endpoints]
Studies reported per year	~22,000
Audit window	90 days ending [Month Year]
Total risks identified	23 (4 Critical, 9 High, 7 Medium, 3 Low)
Annualised exposure to identified Critical risks	\$186,000 to \$410,000

Critical risks at a glance

Ref	Risk	Likely impact (per incident)	Annualised \$ exposure	Closure horizon
C1	PACS reporting list interrupted by single point ISP failure at HQ site (no failover)	4 to 8 hours reporting downtime per event, 2 to 3 events per year observed	\$48,000 to \$96,000	30 days (Sprint Phase 1)
C2	Microsoft 365 backup retention shorter than statutory clinical record period	Inability to restore mailbox or SharePoint data older than 30 days	Compliance / regulatory exposure	30 days (Sprint Phase 1)
C3	Privileged Microsoft 365 admin accounts without Conditional Access enforcement	Tenant wide compromise from a single phished admin credential	\$90,000 to \$250,000 (OAIC 2024 average AU healthcare breach)	7 days (within Audit walkthrough)
C4	Backup restore tests not performed in last 18 months for clinical archive	Untested DR posture; ransomware recovery time unknown	Existential during incident	60 days (Sprint Phase 2)

Sample finding: C1 — single point of failure on primary ISP

What we found

The HQ site at [Address] runs a single fibre service from [ISP A]. Workshop reporting from satellite sites is also tunnelled through HQ, so when HQ loses connectivity the entire reporting list stops. Edge router uptime data for the last 90 days shows 3 unplanned outage events totalling 14 hours, all during business hours. PACS uptime tracker confirms reporting list interrupted on each occasion.

Evidence we collected

- Edge router (FortiGate 60F) WAN1 link state log, 12 February to 12 May
- ISP A network status export, 12 February to 12 May
- PACS event log, study write failures aligned to outage windows
- One radiologist incident report citing "image transfer stalled" during a Tuesday afternoon list

Likely financial impact

- Average reporting list throughput at HQ: 11.4 studies per hour (your data)
- Average billable revenue per study: \$138 (your billing data; MBS items 55700 + 55701 + 55703 averaged)
- Hourly downtime cost (reporting capacity lost, before staff cost): **\$1,573 per hour**
- 90 day observed downtime: 14 hours = **\$22,022 of lost reporting revenue**
- Annualised, assuming current pattern continues: **\$48,000 to \$96,000**

What closes this risk

Sprint Phase 1 (Days 1 to 30): provision a secondary 4G or 5G failover service on a different carrier (Telstra recommended for your geography) with automatic failover at the FortiGate. Ongoing cost: ~\$60 per month. One off cost: ~\$1,200 hardware plus provisioning. **Cost to close ~\$1,920 first year vs \$48,000+ annualised exposure.** Payback inside one outage event.

How findings are scored

Every risk in your full Audit is ranked on:

- **Likelihood** (1 to 5): based on observed frequency in your data, control gaps, and threat patterns from Trucell's monitored fleet of 50 plus imaging practices.
- **Impact** (1 to 5): translated to dollars where possible (lost reporting revenue, breach cost benchmarks, regulatory penalty exposure).
- **Closure horizon**: same week, 30 day Sprint Phase 1, 60 day Phase 2, or 90 day Phase 3.

Critical = Likelihood × Impact ≥ 16. High ≥ 9. Medium ≥ 4. Low = remainder.

What you receive on day 7

This sample page is one of 12 in the full Audit deliverable. The complete report includes:

1. Executive summary and Critical risk table (this page)

2. PACS and RIS uptime evidence review
3. Backup and restore test verification
4. Essential Eight maturity baseline (per strategy scoring)
5. Microsoft 365 governance posture
6. Identity and Conditional Access detail
7. Backup retention vs regulatory and clinical requirement
8. Network resilience and failover
9. Endpoint and patch posture
10. Vendor and integration risk register
11. 90 day remediation plan with named owners
12. One page board summary (forward this to your insurer or AHPRA reviewer the same day)

Our guarantee

If on day seven you tell us the Audit was not worth \$2,500 of your time, we donate \$500 to the **RANZCR Foundation** in your practice's name. We keep no cancellation fee, no reimbursement obligation on your side, and no obligation to talk to us again. The 12 page report is yours to keep regardless.

This sample page is illustrative only. Findings shown are representative of common Audit results across Australian imaging practices and have been generalised to remove identifying information. Your Audit will reflect your specific environment, evidence, and revenue data. Trucell Pty Ltd · ISO 27001:2022 certified · SOC 2 Type II reported · trucell.com.au.