

Contracted network security audit: 64,000 sq ft multi-site campus

Multi-site church campus (name withheld by agreement) · Signed engagement: agreement → on-site assessment → 8-part report → funded decision · Role: assessor and author (implementation was performed separately by a third party)

Outcome: Leadership received plain-English evidence of critical risk, an itemized remediation plan quoted at \$9,900–\$10,700, and acted on it — commissioning a full infrastructure upgrade. Client response on delivery: “Thank you for this detailed report. This is very helpful.”

The Situation

A multi-site campus of roughly 64,000 sq ft was running its entire operation — staff systems, guest WiFi, donated IoT devices, livestream — on consumer-grade networking that had grown one device at a time. Symptoms were the usual ones: dead zones, slowdowns, mystery outages. Nobody knew what was actually on the network. The engagement was contracted under a signed audit agreement with a defined scope, deliverables, and schedule.

What Was Built

- **On-site assessment:** full asset inventory, scan-based discovery, physical inspection of closets, switching, and access points across the campus.
- **Findings that mattered** (each documented with evidence and plain-English impact): the gateway router still used **factory-default credentials; no network segmentation** — staff, guests, and IoT shared one flat network; guest WiFi not isolated from internal resources; donated IoT devices with full network access; the 24-port core switch at capacity with damaged ports; WiFi coverage inadequate for the building.
- **8-part written report suite** built for a non-technical board: options at a glance, executive summary, technical findings, remediation options, cost comparison, equipment pricing, ongoing support options, and cloud alternatives — so leadership could make a funded decision without needing to translate jargon.
- **Tiered remediation quote:** complete managed-infrastructure upgrade priced at \$9,900–\$10,700 plus cabling, with honest lower-cost tiers and the tradeoffs of each spelled out.

Results

- Leadership understood the risk for the first time — the overall HIGH risk rating was supported by findings anyone could verify.
- The report led directly to a funded, full infrastructure upgrade (implemented by a third party of the client’s choosing — the audit was vendor-neutral by design).
- Delivered exactly to the signed agreement: scope, schedule, and an evidence trail from kickoff to board presentation.

Stack & Methods

Methods: network scanning & asset discovery · physical infrastructure inspection · risk rating & prioritization · board-level reporting · vendor-neutral equipment specification · contract-scoped delivery

All work shown is real and operated in production by the author. Names of private organizations are withheld by agreement. Contact via Upwork messages.