**Cybersecurity Case Study: Internal Security Audit**

### **Project Title:**

Internal Cybersecurity Audit – NCRF 2025 Security Access & Device Audit

### **Date of Completion:**

April 13, 2025

### **Role & Contribution:**

IT Auditor / GRC Coordinator / Infrastructure Strategist

### **1. Background:**

With over 100 staff using a mix of outdated personal and company-issued technology, NCRF faced inconsistent performance, Wi-Fi issues, data privacy risks, and reduced productivity. The lack of a formal IT asset registry and no centralized control over devices or software made scaling and securing the organization increasingly difficult. This project was launched to assess and modernize NCRF’s tech usage in alignment with NIST and ISO 27001 standards.

### **2. Objectives:**

* Inventory all office tech and usage patterns across departments
* Determine staff reliance on personal devices for work
* Measure device efficiency and pain points (speed, crashes, connectivity)
* Evaluate access to internal shared drives, Outlook, and critical systems
* Use real data to make executive recommendations for IT transformation

### **3. Methodology:**

* Designed and distributed a Google Form titled “Office Computer Usage & Access Audit” to 150 staff
* Collected detailed metrics on hardware type, software usage, server access, time on devices, and upgrade needs
* Integrated these results into the NCRF Office Computer Research Guide and presented the full report to the Executive Board

### **4. Tools Used:**

* Google Forms (survey data collection)
* Google Sheets (analysis + visuals)
* Google Workspace Admin Console (access review)
* Canva (data visualization and layout for presentation)
* Label Maker + Barcodes (device tracking and organization)

### **5. Key Findings:**

* **72% of staff** rely on personal laptops for work
* **53% reported Wi-Fi reliability issues**; several had no ethernet access
* **Over 50% experienced frequent slowdowns, crashes, or storage problems**
* Only **6% of staff used Microsoft Outlook**, despite the organization paying for licenses
* Staff using Adobe tools faced major slowness on Dell machines, interfering with design workflows

"My Adobe tools crash constantly — I can’t work like this." "It takes five minutes to open an email." "I use my phone because the computer barely runs."

### **6. Remediation Plan:**

* Developed a $40K infrastructure proposal for mini PCs, travel laptops, and networking upgrades
* Cleaned and organized the tech room with labeled, barcoded equipment
* Created a quarterly IT audit protocol using Google Sheets and Trello for task tracking
* Recommended upgrades to mesh Wi-Fi, new modems, and centralized router control with VLANs
* Trained staff on digital hygiene, shared drives, and access responsibilities

### **7. Results & Lessons Learned:**

* Executives approved a phased rollout of standard laptops and mini PCs
* Staff satisfaction increased immediately with faster, more stable setups
* Expos are now supported with reliable travel kits, reducing onsite tech friction
* NCRF's GRC posture improved with new policies for device use, login hygiene, and endpoint tracking

### **8. Portfolio Attachments:**

* ✅ [Google Form View-Only Link (Private)]
* ✅ PDF Summary of Survey Results
* ✅ [NCRF Office Computer Research Guide Report – 2025]
* ✅ Screenshots of Barcode Labels, Charts, and Onboarding Templates

### **9. Skills Demonstrated:**

* GRC-aligned Audit & Asset Management
* Risk Assessment & Policy Enforcement
* Hardware Lifecycle Planning & Procurement Strategy
* Executive Presentation & Strategic Communication
* Technical Documentation & Ticketing System Design
* ISO 27001 / NIST Framework Mapping

*Prepared by:* Dakarai Willis  
*Email:* Dakarai@ncrfoundation.org  
*LinkedIn:* [www.linkedin.com/in/dakarai-willis](http://www.linkedin.com/in/dakarai-willis)

