SIMULATED SYSTEM AUDIT CASE STUDY - DELTAFIX SERVICES LTD.

Executive Summary

This report presents the results of a comprehensive system audit conducted for DeltaFix Services Ltd., a small service enterprise. The audit aimed to evaluate IT infrastructure, assess security risks, improve operational efficiency, and ensure data protection.

Key outcomes of the audit include:

- Identification of critical vulnerabilities in network security and data management
- Recommendations for cost-effective improvements
- Simulated implementation results demonstrating reduced downtime and enhanced data security

Client Background

Client Name: DeltaFix Services Ltd.

Industry: Appliance Installation & Repair Services

Staff Strength: 8 employees

IT Assets:

- 5 Windows 11 PCs
- 2 laptops
- 3 Android devices
- 1 Wi-Fi router
- Shared external hard drive
- Microsoft Excel for records
- WhatsApp Business for communications

Audit Objectives

1. Evaluate hardware and software health
2. Assess network and cybersecurity risks
3. Review data storage and backup procedures
4. Identify operational inefficiencies
5. Provide actionable recommendations

Audit Scope

Included: Workstations, laptops, network, business applications, user practices.

Excluded: Third-party cloud providers or ISP infrastructure.

Audit Methodology

Tools & Techniques:

- Windows Security Center & Event Viewer
- Command Prompt (ipconfig, netstat)
- Nmap for network scanning
- Manual configuration review
- User interviews
- Backup test and restore exercises

Audit Steps:

1. Asset inventory
2. Vulnerability scanning
3. Password & access policy review
4. Network security assessment
5. Backup & data protection review
6. Risk assessment
7. Recommendations & implementation planning

Findings

Hardware:

Issue	Risk Level	Observation
Aging HDDs on 2 PCs	Medium	Slow performance
No UPS	High	Risk of power loss
Shared flash drives	High	Malware risk

Software:

Issue	Risk Level	Observation
Outdated Windows OS	High	Vulnerable to exploits
No antivirus on 2 PCs	High	Malware infection risk

Unlicensed software	High	Legal & security risk

Network Security:

Issue	Risk Level	Observation
Default router password	Critical	Easily exploitable
No firewall rules	High	Open ports exposed
Single Wi-Fi for staff & guests	Medium	Unauthorized access possible

Security Practices:

Issue	Risk Level	Observation
Weak passwords	High	Easily guessable
No structured backups	Critical	Data loss risk
Lack of access controls	Medium	Employees have unrestricted access

Data Management:

Issue	Risk Level	Observation
Data stored locally only	High	Loss if system fails
No encryption	Medium	Data exposure
Manual tracking in Excel	Medium	Errors and inefficiencies

Risk Assessment

Risk	Impact	Likelihood	Priority
Data loss	Severe	High	Critical
Malware infection	High	High	Critical
Unauthorized access	High	Medium	High
Operational downtime	Medium	High	High

Recommendations

Immediate (0–1 month):

- Change default router password
- Install antivirus
- Enable automatic updates
- Weekly backups
- Remove unlicensed software

Short Term (1–3 months):

- Purchase UPS
- Encrypted backup storage

- Role-based user accounts
- Firewall rules
- Staff cybersecurity training

Long Term (3–6 months):

- Cloud backup migration
- Implement CRM system
- Network segmentation
- Password manager
- IT policy documentation

Implementation Plan

Task	Cost Estimate	Duration
Antivirus licenses	₦30,000	1 day
UPS units	₦120,000	2 days
Encrypted backup drive	₦45,000	1 day
Staff training	₦0 (internal)	2 days
Cloud backup setup	₦15,000/month	1 day

Total Initial Cost ≈ ₦210,000

Simulated Results After Implementation

Metric	Before Audit	After Implementation
System downtime	8 hrs/month	3 hrs/month
Malware incidents	4/month	0
Data loss events	2/year	0
Customer response time	Slow	Faster
Security posture	Low	Medium-High

Lessons Learned

- Small businesses are vulnerable to cybersecurity risks
- Structured audits improve efficiency
- Low-cost controls provide high impact
- Staff awareness is critical

Conclusion

The audit demonstrates that even basic IT assessments can uncover critical vulnerabilities and guide actionable improvements. Following these practices prepares small businesses for secure, efficient, and resilient operations.

Skills Demonstrated

- IT Infrastructure Auditing
- Risk Assessment & Mitigation
- Network & Cybersecurity Analysis
- Data Backup Strategy Design
- Windows Administration
- Technical Documentation & Reporting