Cybersecurity Internal Audit Case Study

CASE STUDY

Strengthening Cybersecurity

THROUGH BETTER INTERNAL AUDITS

Visibility today. Protection tomorrow.

THE SITUATION

A manufacturing company with multiple facilities believed its cybersecurity program was well managed. Policies existed, annual security training was completed, and external vulnerability scans were conducted.

However, an internal cybersecurity audit revealed several hidden risks:

- Former employees still had active system accounts.
- Multi-factor authentication was not consistently enforced.
- Critical patches were delayed by several months.
- Backup restoration testing had not been performed.

ACTIONS TAKEN

The company implemented a stronger, risk-focused approach:

- Implemented a risk-based cybersecurity audit schedule
- Established monthly access reviews
- Automated patch status reporting
- Conducted backup recovery testing
- Enhanced employee phishing awareness training

RESULTS WITHIN 12 MONTHS

- Reduced unauthorized account exposure by **90%**
- Improved patch compliance rates
- Increased phishing awareness across the workforce
- Strengthened customer confidence during supplier assessments
- Improved readiness for future cybersecurity certification efforts

KEY TAKEAWAY

The organization wasn't lacking policies—it was lacking visibility into whether controls were actually working.

Effective cybersecurity audits bridge the gap between documented procedures and real-world protection.

NCK CONSULTING

STRONGER AUDITS.
STRONGER SECURITY.
STRONGER BUSINESS.

www.nckconsulting.com
info@nckconsulting.com
330-327-3060

CYBERSECURITY INTERNAL AUDIT EFFECTIVENESS CHECKLIST

Use this quick assessment to evaluate your cybersecurity audit program.

GOVERNANCE & PLANNING

- ☐ Cybersecurity risks are included in the audit program
- ☐ Critical systems receive increased audit attention
- ☐ Audit frequency is based on risk
- ☐ Security-related incidents influence audit planning

ACCESS MANAGEMENT

- ☐ User accounts are periodically reviewed
- ☐ Terminated employee accounts are removed promptly
- ☐ Privileged access is monitored
- ☐ Multi-factor authentication is implemented where appropriate

TECHNICAL CONTROLS

- ☐ Systems receive timely security updates
- ☐ Vulnerability scans are reviewed and tracked
- ☐ Security configurations are periodically verified
- ☐ Backup processes are tested

EMPLOYEE AWARENESS

- ☐ Security awareness training is conducted regularly
- ☐ Phishing susceptibility is evaluated
- ☐ Employees understand reporting procedures
- ☐ Security responsibilities are clearly communicated

CORRECTIVE ACTION MANAGEMENT

- ☐ Security findings receive root cause analysis
- ☐ Corrective actions have assigned owners
- ☐ Effectiveness is verified before closure
- ☐ Repeat findings are tracked and analyzed

LEADERSHIP OVERSIGHT

- ☐ Cybersecurity results are reviewed by management
- ☐ Trends and recurring issues are monitored
- ☐ Cybersecurity risks are discussed during management reviews
- ☐ Resources are allocated to address significant risks