SAMPLE CLIENT DELIVERABLE

# Cyber Readiness Assessment Report

A practical, business-focused security review prepared by NodeVera Cyber IT & Services for small and growing organizations that want to reduce cyber risk without unnecessary complexity.

Business Email Security | Payment Fraud Prevention | Staff Awareness | Data Protection | Incident Readiness

PREPARED FOR
**Sample SME Client**

PREPARED BY
**NodeVera Cyber IT & Services**

REPORT TYPE
**Sample Readiness Report**

## What this sample shows

This sample demonstrates the structure, clarity and practical action plan a client can expect after a NodeVera cyber readiness review. A real client report would be based on interviews, evidence review and agreed assessment scope.

## NodeVera approach

We focus on the risks that most often affect SMEs: email compromise, payment fraud, weak access control, staff mistakes, exposed business data and lack of response planning.

DOCUMENT GUIDE

# Table of Contents



## Important note

This is a sample report for demonstration only. It is not a certification, penetration test, legal opinion or formal data protection audit. A real assessment should be adapted to the client's industry, size, tools, staff count, operating process and evidence provided.

SECTION 1

# Report Overview and Sample Client Context

## Purpose of the review

The purpose of this cyber readiness assessment is to identify practical security gaps that could lead to business email compromise, payment fraud, staff-related incidents, data exposure, operational disruption or reputational damage.

The report converts those risks into clear actions the business can start implementing within 30 days.

## Sample client profile

| | |
|---|---|
| **Business type** | Growing SME with 18 staff |
| **Digital tools** | Business email, website, WhatsApp, shared cloud drive |
| **Key concern** | Email safety, staff scams and payment approval process |
| **Assessment mode** | Remote review and guided evidence request |

## NodeVera assessment objective

NodeVera does not only point out problems. The objective is to help the business understand what can go wrong, which issues matter first, who should own each fix and what simple controls can reduce real business risk quickly.

**9**
Risk domains reviewed

**30**
Day action roadmap

**6**
Priority findings included

SECTION 2

# Executive Summary

| 54% | High | 30 |
|---|---|---|
| Overall readiness score | Payment fraud exposure | Days to fix priority gaps |

## Summary conclusion

The sample business shows moderate cyber readiness. Basic digital operations are in place, but there are important weaknesses around multi-factor authentication, staff awareness, shared access, former staff access removal, payment verification and backup testing.

The most urgent business risks are not highly technical. They are practical operational risks that can lead to money loss, account takeover, fake payment instruction, customer trust damage and business disruption.

## Top strengths observed

- Business uses company email instead of only personal email.
- There is a named person responsible for admin accounts.
- Important documents are stored digitally and can be reviewed.
- Management is aware that staff mistakes can create risk.

## Top weaknesses observed

- MFA is not consistently enabled on all critical accounts.
- Payment approval process depends too much on trust and WhatsApp.
- Former staff access review is not documented.
- Backups exist, but restore testing is not confirmed.

## Readiness interpretation

**54% readiness** means the business has started using some basic controls, but several high-impact gaps remain. NodeVera recommends immediate fixes within 7 days for email and payment controls, followed by structured improvements within 30 days.

SECTION 3

# Assessment Scope and Scoring Method

## Assessment scope

This sample review focuses on the areas that commonly create the biggest risk for SMEs: email accounts, staff behavior, payment workflow, devices, cloud tools, website/admin access, business data, backup readiness and incident response.

| Domain | What NodeVera reviews | Why it matters |
|---|---|---|
| Email and accounts | MFA, admin roles, recovery settings, password practices | Email compromise can lead to fake invoices and payment redirection. |
| Staff awareness | Phishing knowledge, scam reporting, payment instruction caution | Staff mistakes are often the entry point for scams. |
| Payment controls | Approval steps, call-back verification, vendor changes | Money loss can happen without malware or hacking. |
| Devices and access | Device locks, antivirus, shared logins, former staff access | Weak access control increases exposure when staff change roles or leave. |
| Data and backup | Customer data handling, backup frequency, restore testing | Poor backup and data control can disrupt operations and damage trust. |
| Incident response | Escalation process, evidence collection, immediate actions | Fast action reduces damage when something suspicious happens. |

## Scoring method

Each control is scored based on whether it is present, documented, consistently used and confirmed by evidence. Higher scores mean lower immediate business exposure.

## Priority method

Findings are prioritized by likelihood, business impact, ease of exploitation and how quickly the business can reduce the risk.

SECTION 4

# Risk Snapshot by Domain

| Area | Score | Risk level | What this means | Priority |
|---|---|---|---|---|
| Email and Accounts | 45% | High | MFA and recovery protection need urgent improvement. | Fix in 7 days |
| Payment Fraud Controls | 38% | High | Fake invoice or changed account details may not be caught early. | Fix in 7 days |
| Staff Awareness | 50% | Medium | Staff need practical scam and reporting training. | Fix in 14 days |
| Devices and Access | 58% | Medium | Access cleanup and device baseline are incomplete. | Fix in 30 days |
| Data Protection | 52% | Medium | Data handling is informal and policy evidence is limited. | Fix in 30 days |
| Backup and Recovery | 60% | Medium | Backup exists but restore testing is not proven. | Fix in 30 days |
| Website and Public Channels | 64% | Medium | Ownership and admin access should be reviewed. | Fix in 30 days |
| Incident Response | 42% | High | No clear process for reporting and containing incidents. | Fix in 14 days |

## NodeVera interpretation

The business should not start with expensive tools. The first priority is to fix high-impact basics: MFA, payment verification, access cleanup, staff reporting, backup testing and a simple incident response plan.

SECTION 5

# Priority Findings and Action Plan

| # | Finding | Severity | Business impact | Recommended action |
|---|---|---|---|---|
| 1 | MFA is not enforced on all critical accounts. | High | Email takeover and payment fraud. | Enable MFA and protect recovery options. |
| 2 | Payment changes are approved without independent verification. | High | Funds may be sent to attacker-controlled accounts. | Create payment call-back and vendor change procedure. |
| 3 | No documented staff scam reporting process. | Medium | Suspicious activity may be reported late. | Introduce a simple reporting channel and response steps. |
| 4 | Former staff access removal is informal. | Medium | Ex-staff may retain access to business tools. | Create offboarding checklist and quarterly access review. |
| 5 | Backup restore testing is not confirmed. | Medium | Business may not recover quickly after data loss. | Test restore and document backup owner. |
| 6 | Incident response plan is missing. | High | Confusion during compromise can increase loss. | Create 1-page incident response guide. |

### First 7 days

Fix MFA, payment verification, recovery settings and admin accounts.

### First 14 days

Train staff, create reporting path and document emergency actions.

### First 30 days

Review access, test backups, improve policies and confirm ownership.

SECTION 6

# Detailed Findings

## Finding 1: MFA is not enforced on all critical accounts

High

**Observation**

Some business email, cloud storage and admin accounts may still allow password-only access.

**Business impact**

An attacker who steals one password may access invoices, customer records or internal messages.

**Evidence to confirm**

Admin screenshots showing MFA status, recovery email, admin roles and last login activity.

**Recommended action**

Enable MFA for owners, finance staff, administrators and all accounts with access to sensitive data.

**Owner:** Business owner / IT lead. **Timeframe:** 7 days. **Quick win:** Start with email admin and finance accounts.

## Finding 2: Payment changes are not independently verified

High

**Observation**

Payment requests, vendor bank detail changes or invoice updates may be approved through email or WhatsApp alone.

**Business impact**

Attackers can impersonate vendors or executives and redirect payment to another account.

**Evidence to confirm**

Current payment approval process, sample invoice flow and who can approve account changes.

**Recommended action**

Use call-back verification and two-person approval for new vendor accounts or changed bank details.

**Owner:** Finance lead / business owner. **Timeframe:** 7 days. **Quick win:** No bank detail change should be approved only by message.

SECTION 6 CONTINUED

# Detailed Findings

## Finding 3: Staff do not have a clear scam reporting process

Medium

**Observation**

Staff may not know who to contact when they click a suspicious link, receive a fake invoice or notice unusual account activity.

**Business impact**

Late reporting gives attackers more time to access accounts, send messages or change payment instructions.

**Evidence to confirm**

Staff awareness materials, internal reporting channel and previous incident handling examples.

**Recommended action**

Create a one-page scam reporting guide and train staff on examples relevant to the business.

**Owner:** Operations / HR. **Timeframe:** 14 days. **Quick win:** Create a WhatsApp/email reporting contact for suspicious messages.

## Finding 4: Former staff access removal is informal

Medium

**Observation**

The business does not have a documented checklist for disabling email, cloud drive, website, social media and vendor access when staff leave.

**Business impact**

Former staff may retain access to documents, customer records, admin panels or business channels.

**Evidence to confirm**

List of active users, former staff list, shared accounts and admin roles in cloud tools.

**Recommended action**

Create an offboarding checklist and review all active users every quarter.

**Owner:** HR / admin / IT lead. **Timeframe:** 30 days. **Quick win:** Review accounts of the last five staff who left.

SECTION 6 CONTINUED

# Detailed Findings

## Finding 5: Backup restore testing is not confirmed

Medium

**Observation**

Some files may be backed up, but there is no clear evidence that the business can restore important files quickly.

**Business impact**

Data loss, accidental deletion, ransomware or device failure could interrupt operations for days.

**Evidence to confirm**

Backup location, backup owner, frequency, last restore test and list of critical business files.

**Recommended action**

Run a restore test for key files and document recovery steps.

**Owner:** Operations / IT lead. **Timeframe:** 30 days. **Quick win:** Restore one important folder to confirm the backup works.

## Finding 6: Incident response plan is missing

High

**Observation**

The business does not have a written process for what to do when email, WhatsApp, payment or data exposure issues occur.

**Business impact**

Confusion can cause delayed password resets, poor evidence handling and slow customer or bank notification.

**Evidence to confirm**

Incident contact list, decision owner, bank contact, email admin access and escalation plan.

**Recommended action**

Create a one-page incident response guide covering first actions, contacts, evidence and communication.

**Owner:** Business owner / operations lead. **Timeframe:** 14 days. **Quick win:** Document who must be called in the first 30 minutes.

SECTION 7

# 30-Day Improvement Roadmap

## Days 1-7

- Enable MFA on admin, owner and finance accounts.
- Review recovery email and phone numbers.
- Pause payment changes without call-back verification.
- Identify all shared accounts and admins.

## Days 8-14

- Run staff scam awareness session.
- Create suspicious message reporting procedure.
- Draft incident response guide.
- Create vendor bank detail change procedure.

## Days 15-30

- Complete access review for staff and former staff.
- Test backup restore.
- Review website/domain ownership.
- Prepare data handling and privacy documents.

## Recommended implementation sequence

NodeVera recommends fixing high-impact controls first instead of trying to do everything at once. The first target should be account protection and payment verification because those can directly reduce the chance of money loss.

| Action | Owner | Target | Success measure |
|---|---|---|---|
| Enable MFA on critical accounts | IT/admin owner | 7 days | All admin and finance accounts show MFA enabled. |
| Create payment verification rule | Finance lead | 7 days | No vendor account change without independent confirmation. |
| Train staff on scam reporting | Operations/HR | 14 days | Staff know where and how to report suspicious messages. |
| Test backup restore | Operations/IT | 30 days | One critical folder restored successfully and documented. |

SECTION 8

# Implementation Tracker

This tracker helps management turn the report into action. Each task should have one accountable owner and a clear deadline.

| | Control improvement | Priority | Owner | Status |
|---|---|---|---|---|
| ☐ | Enable MFA on all critical business email accounts. | High | | |
| ☐ | Review and protect account recovery options. | High | | |
| ☐ | Document payment verification procedure for vendor changes. | High | | |
| ☐ | Create suspicious message reporting channel for staff. | Medium | | |
| ☐ | Run staff awareness training using practical Nigerian business scam examples. | Medium | | |
| ☐ | Create staff exit and access removal checklist. | Medium | | |
| ☐ | Review website, domain, hosting and social media admin access. | Medium | | |
| ☐ | Run a backup restore test and document recovery process. | Medium | | |
| ☐ | Create one-page incident response guide and contact list. | High | | |

## Management review note

The business should review progress weekly until all high-priority actions are closed. Medium-priority items should be tracked until completion, not left as informal intentions.

SECTION 9

# Evidence Request Checklist

In a real engagement, NodeVera may request evidence like the items below. The goal is to verify controls without asking for unnecessary sensitive information.

## Email and identity

- List of business email users and admins.
- MFA status screenshot.
- Recovery settings screenshot.
- Recent suspicious email examples if available.

## Payment process

- Payment approval steps.
- Vendor bank detail change process.
- Who can approve payments.
- Recent fraud or near-miss examples if any.

## Devices and access

- Staff device list.
- Shared account list.
- Former staff access removal evidence.
- Website and social media admin list.

## Data and recovery

- Where customer or business records are stored.
- Backup frequency.
- Last restore test.
- Any privacy notice or data handling policy.

## Security note

NodeVera does not require client passwords for a readiness review. Where access confirmation is needed, the client can share screenshots, admin summaries or join a guided screen-share session.

SECTION 10

# Recommended NodeVera Next Steps

## Immediate recommendation

The sample client should start with the **Business Email and Payment Fraud Protection** package because the highest risks relate to account compromise and payment redirection.

**Starting price:** NGN 150,000. Final quote depends on number of accounts, staff count, systems involved and urgency.

## Secondary recommendation

After account and payment controls are improved, the business should book **Staff Scam Awareness Training** to reduce repeat exposure from phishing, WhatsApp scams, fake invoices and social engineering.

**Starting price:** NGN 200,000 per session.

## How NodeVera can help

NodeVera can help management confirm priority risks, implement practical controls, train staff, review access, improve payment verification, prepare documentation and provide ongoing advisory support.

| Need | Recommended NodeVera service | Expected outcome |
|---|---|---|
| Not sure where to start | Cyber Readiness Starter | Clear risk picture and action plan. |
| Email or payment risk | Business Email and Payment Fraud Protection | Reduced account takeover and fake payment risk. |
| Staff mistakes | Staff Scam Awareness Training | Better staff recognition and reporting of scams. |
| Ongoing guidance | Monthly Cyber Advisor | Practical monthly support without hiring full-time security staff. |

## Contact

NodeVera Cyber IT & Services
Website: nodeveracyber.com
Email: info@nodeveracyber.com
Phone/WhatsApp: +234 703 562 2388