Own Layer

Cyber intelligence for SMEs

Deep Review

Northstar Services Ltd

Illustrative sample report

REPORT STATUS	**EXAMPLE ONLY - NO LIVE CHECKS WERE RUN**
PREPARED	24 September 2026
SCOPE	One UK business, one primary domain and authorised business-control evidence
SERVICE	Own Layer Deep Review - pilot scope

A clearer way to manage cyber security.

This sample shows the standard, structure and clarity intended for a paid review. All company details, evidence and findings are fictional. Real reports identify the exact source, date and scope of every completed check.

hello@ownlayer.co.uk

+44 7448 950326

01 / EXECUTIVE VIEW

The short version.

Northstar has useful foundations, but six items need action or confirmation. The most important concerns are exposed historic account data and the way supplier bank-detail changes are approved. Nothing in this sample proves that the business has been breached.

16	6	2	5
areas reviewed	actionable findings	deal with first	Cyber Essentials areas

What matters first

01	**Check the two exposed historic accounts**	Confirm whether the accounts still work, reset credentials safely and verify multi-factor authentication.
02	**Strengthen payment-change approval**	Verify every new or changed bank account through a trusted second channel before payment.
03	**Move DMARC beyond monitoring**	Confirm every genuine email sender, review reports and move safely towards an enforcing policy.
04	**Close evidence gaps**	Confirm former-staff access removal, a recent restore test and the status of legacy TLS support.

What is already working

The sample evidence shows a valid SPF record, working HTTPS, current certificates, administrator MFA and managed endpoint protection. These positives reduce risk, but they do not cancel the open findings.

OWN LAYER VIEW	**Proceed with a 30-day resolution plan, then recheck the public controls and retain closure evidence in the Protection Record.**

02 / REVIEW AREAS

The six parts of the review.

Our checks follow NCSC guidance for small businesses. We use our own words and add an outside view of the signals bad actors can see without logging in.

#	AREA	PLAIN-ENGLISH AIM	EVIDENCE
01	**Backing up your data**	Confirm what is protected, who can reach it and whether a real restore has been tested.	Restore test and backup settings
02	**Protecting against malware**	Check that business devices have suitable protection and that warnings are acted on.	Protection status and exceptions
03	**Keeping devices safe**	Confirm supported software, timely updates and safer everyday settings.	Device list, update status and settings
04	**Passwords and two-step login**	Review important accounts, access levels, leavers and two-step login.	Account and access evidence
05	**Avoiding phishing**	Review email trust, payment changes and how staff verify unusual requests.	Email controls and working procedures
06	**Our outside view**	Check email that can be faked, leaked staff passwords, lookalike domains and visible website weaknesses.	Public and authorised intelligence

Guidance link

NCSC Small Business Guide: https://www.ncsc.gov.uk/collection/small-business-guide

Own Layer is not claiming NCSC approval or endorsement. The guide provides a practical baseline; the Deep Review adds evidence, priorities and an outside view.

03 / SCOPE

What was reviewed - and what was not.

A good report shows its boundaries. Each area below has a result only when the named evidence was obtained. Simulated licensed results are labelled clearly in this sample.

#	CHECK AREA	EVIDENCE	STATUS
01	**Backing up data**	Restore evidence and settings	**Action needed**
02	**Malware protection**	Device protection evidence	**Complete**
03	**Keeping devices safe**	Updates, support and secure settings	**Partly complete**
04	**Passwords and two-step login**	Accounts, MFA and leavers	**Action needed**
05	**Avoiding phishing**	Email and payment procedures	**Action needed**
06	**Outside view: email identity**	SPF, DMARC and mail policies	**Complete**
07	**Outside view: leaked accounts**	Simulated licensed sources	**Illustrative**
08	**Outside view: lookalike domains**	DNS, certificates and brand evidence	**Complete**
09	**Outside view: website weaknesses**	TLS, headers and Observatory	**Complete**
10	**Domain and DNS**	Public DNS, DNSSEC and CAA	**Complete**
11	**Mail routing**	MX records	**Complete**
12	**Public names**	Certificate Transparency	**Complete**
13	**External services**	Authorised discovery	**Partly complete**
14	**Known vulnerabilities**	CISA KEV, EPSS and vendor data	**Partly complete**
15	**Reputation warnings**	Keyed intelligence	**Complete**
16	**Cyber Essentials readiness**	Authorised client evidence	**Partly complete**

Important boundary

No password testing, exploitation, mailbox reading, device installation or destructive scanning is included. Credential and dark-web intelligence requires appropriate access, licensing and proof that the client controls the domain. Cyber Essentials certification is completed by an IASME-licensed Certification Body, not by this report.

04 / PRIORITY FINDINGS

Deal with these first.

Historic work accounts appear in exposure data [redacted]

WHAT WE FOUND	The simulated licensed result contains two old Northstar work addresses connected with historic breach or stealer-log records.
WHAT COULD HAPPEN	If either account still works, an attacker could try an old password, target the employee with a convincing message or use the information to support fraud.
EVIDENCE	Illustrative licensed intelligence result. In a real report the provider, event date, affected account, first-seen date and retrieval date would be recorded. Password values would not be copied into the report.
WHAT SHOULD HAPPEN	Confirm whether each account is active. Reset credentials through the normal admin process, revoke old sessions, verify MFA and review recent sign-in history.
OWNER / PROOF	Microsoft 365 administrator - target: 48 hours Export showing account state, password reset, session revocation, MFA status and sign-in review. Recheck the source after closure.
TECHNICAL DETAIL	Authorised HIBP domain evidence and/or SOCRadar intelligence may be used subject to verification and commercial terms. Exposure data does not prove that the current password works or that the account was used maliciously.

04 / PRIORITY FINDINGS - CONTINUED

Deal with this first.

Supplier bank-detail changes rely too heavily on email [redacted]

WHAT WE FOUND	The fictional finance interview states that a bank-detail change can be approved from an email thread without an independent call to a known number.
WHAT COULD HAPPEN	A fraudster who controls or imitates a supplier mailbox could redirect a genuine payment.
EVIDENCE	Illustrative management interview and draft payment procedure. No bank information or payment records were collected.
WHAT SHOULD HAPPEN	Require a second person and a known-number callback for every new or changed payee. Never use contact details contained only in the change request.
OWNER / PROOF	Finance director - target: 7 days Approved procedure, staff acknowledgement and one redacted test record showing the separate verification step.
TECHNICAL DETAIL	This is a business-control finding, not a claim that fraud has occurred. The control is intended to reduce business email compromise and invoice-redirection risk.

05 / FURTHER FINDINGS

Important work for the next 30 days.

DMARC is monitoring, not enforcing

RESOLVE NEXT

WHAT WE FOUND	A DMARC record is published with p=none. Reports can be collected, but receiving systems are not asked to quarantine or reject failing messages.
WHAT COULD HAPPEN	A convincing message that pretends to come directly from the domain may have a better chance of reaching a customer or employee.
EVIDENCE	Public DNS TXT response for _dmarc.northstar.example at the fictional review time.
WHAT SHOULD HAPPEN	Inventory every genuine sender, review DMARC reports, correct alignment and move gradually towards quarantine and reject without disrupting valid mail.
OWNER / PROOF	Email provider - target: 30 days Before-and-after DNS evidence, report analysis and test messages from every genuine sending service.
TECHNICAL DETAIL	Example record: v=DMARC1; p=none; rua=mailto:dmarc@northstar.example. An enforcing policy should follow analysis, not be changed blindly.

05 / FURTHER FINDINGS - CONTINUED

Access should be closed - and proved.

Former-staff access removal is not evidenced

RESOLVE NEXT

WHAT WE FOUND	Management believes the leaver account was closed, but no dated record shows which cloud services, groups, shared mailboxes or forwarding rules were checked.
WHAT COULD HAPPEN	A forgotten account or forwarding rule could retain access to email, files or customer information.
EVIDENCE	Illustrative leaver checklist and administrator interview. The evidence was incomplete.
WHAT SHOULD HAPPEN	Run a documented leaver review across email, file storage, finance, CRM, password manager, domain registrar and remote support tools.
OWNER / PROOF	Operations lead and IT provider - target: 7 days Signed leaver record plus administrator exports showing account block, session revocation, group removal and forwarding-rule review.
TECHNICAL DETAIL	The report does not state that access remains open. It states that closure could not be proved from the evidence supplied.

05 / FURTHER FINDINGS - CONTINUED

Remove avoidable technical risk.

Old TLS versions are shown as enabled

RESOLVE NEXT

WHAT WE FOUND	The simulated specialist check reports TLS 1.0 and TLS 1.1 support on the public website.
WHAT COULD HAPPEN	Older connection methods can weaken protection and may fail customer, insurer or tender expectations.
EVIDENCE	Illustrative external TLS configuration result. A real report records the tested host, IP, scan time and source result.
WHAT SHOULD HAPPEN	Ask the hosting provider to confirm compatibility, disable old protocol support and retest from outside the network.
OWNER / PROOF	Website host - target: 14 days Provider change ticket and a clean external retest showing only approved protocol versions.
TECHNICAL DETAIL	A TLS finding must be reproduced against the correct host and service. The free check confirms HTTPS reachability but does not make this deeper protocol claim.

05 / FURTHER FINDINGS - CONTINUED

A backup is only useful if it restores.

A recent backup restore test is not available

RESOLVE NEXT

WHAT WE FOUND	Backups are reported as successful, but the latest restore evidence in the fictional review is fourteen months old.
WHAT COULD HAPPEN	A backup can appear healthy yet fail when the business urgently needs files or systems restored.
EVIDENCE	Illustrative backup console screenshot and management interview.
WHAT SHOULD HAPPEN	Choose one important service, run a controlled restore test and record the result, time taken, gaps and next test date.
OWNER / PROOF	IT provider and business owner - target: 30 days Dated restore-test record with the restored item, outcome, recovery time and approval by the business owner.
TECHNICAL DETAIL	Backup success and recovery readiness are different claims. This finding concerns missing restore evidence, not proof that backups are unusable.

06 / CYBER ESSENTIALS

Preparation view - not certification.

Cyber Essentials is built around five technical controls. The current NCSC requirements are version 3.3 for applications created from 27 April 2026. This example shows how Own Layer would organise evidence before formal assessment.

CONTROL	VIEW	EVIDENCE / NEXT STEP
Firewalls (control internet connections)	**Partly ready**	Business routers identified; remote administration evidence still required.
Secure configuration (safe settings)	**Action needed**	Default accounts and unnecessary services need a documented review.
Security update management (keep software updated)	**Partly ready**	Managed devices have a policy; unsupported software and cloud responsibility need confirmation.
User access control (who can log in)	**Action needed**	Leaver evidence is incomplete; MFA should be confirmed for every supported cloud service.
Malware protection (virus protection)	**Ready to evidence**	Managed endpoint protection is reported; current coverage and exceptions need export evidence.

Recommended route

1. Agree the assessment scope. 2. Close the leaver, configuration and evidence gaps. 3. Complete the official question set. 4. Use an IASME-licensed Certification Body for assessment and certification. 5. Keep the Protection Record current after certification.

IMPORTANT	**Own Layer can support preparation, evidence gathering and remediation coordination. This sample does not claim that Own Layer currently issues Cyber Essentials certificates.**

07 / RESOLUTION PLAN

Who does what - and how closure is proved.

A recommendation is not finished work. Each action remains open until the agreed evidence is supplied and the relevant check is repeated.

PRI	ACTION	OWNER	TARGET	CLOSURE EVIDENCE	STATUS
P1	**Historic exposed accounts**	M365 admin	48 hours	Account export, reset, MFA and sign-in review	**Open**
P1	**Payment-change verification**	Finance director	7 days	Approved procedure and redacted test	**Open**
P2	**Leaver access evidence**	IT provider	7 days	Leaver export and forwarding-rule review	**Open**
P2	**Legacy TLS support**	Website host	14 days	Change ticket and external retest	**Open**
P2	**DMARC enforcement plan**	Email provider	30 days	Sender inventory, reports and DNS retest	**Open**
P2	**Backup restore evidence**	IT provider	30 days	Dated restore-test record	**Open**
P3	**Cyber Essentials evidence pack**	Operations lead	45 days	Completed scope and evidence register	**Planned**

Closure rule

Own Layer records the person responsible, target date, evidence supplied, reviewer and recheck result. A screenshot alone may be insufficient if it does not identify the relevant system, date or setting. The business or its IT provider remains responsible for approving and safely implementing changes.

The Protection Record

The final record should show the original finding, business consequence, agreed action, owner, target, provider response, before-and-after evidence and verification outcome. It can then support directors, insurers, customers, tenders and future Cyber Essentials preparation.

08 / SOURCES AND LIMITS

Transparent evidence, stated plainly.

Own Layer does not treat a missing record, a similar domain or an intelligence mention as proof of compromise. Findings are weighted by source, age, confidence and business context.

SOURCE	USED FOR	REFERENCE
Google Public DNS	Public DNS evidence	https://dns.google/
MDN HTTP Observatory	Website security headers	https://developer.mozilla.org/en-US/observatory/
Certificate Transparency / Cert Spotter	Public certificate names and expiry records	https://sslmate.com/certspotter/
CISA Known Exploited Vulnerabilities	Known exploitation catalogue	https://www.cisa.gov/known-exploited-vulnerabilities-catalog
FIRST EPSS	Probability context for published vulnerabilities	https://www.first.org/epss/
Have I Been Pwned	Authorised domain exposure evidence	https://haveibeenpwned.com/API/v3
SOCRadar External Threat Assessment	External and dark-web intelligence input	https://socradar.io/free-tools/threat-reports/external-threat-assessment
NCSC Cyber Essentials v3.3	Five control requirements	https://www.ncsc.gov.uk/cyberessentials/resources

Use of third-party intelligence

Third-party names are shown to explain possible evidence sources. Their inclusion does not imply endorsement, partnership or a live integration. A real engagement would state which source was actually used and whether its terms permit the intended client use. Raw third-party reports are not presented as Own Layer's work.

What the report cannot promise

No review can prove that an organisation is completely secure. Public data can be incomplete or stale. A clean result from one source means only that the source returned no matching evidence at that time. Material technical changes should be implemented by an appropriately competent provider, tested and backed out safely if necessary.

SEE THE RISK. FINISH THE WORK. PROVE THE PROTECTION.

Own Layer - independent cyber review, Cyber Essentials preparation and resolution evidence for growing UK businesses.