SAMPLE

BLC Blue Line Cyber

SAMPLE SECURITY ASSESSMENT

Cybersecurity Assessment & Gap Analysis

A demonstration of the deliverable Blue Line Cyber provides to small municipalities — prepared for a fictional client to illustrate our methodology, findings format, and remediation roadmap.

PREPARED FOR
Village of Cedar Hollow, IL (fictional)

PREPARED BY
Blue Line Cyber LLC

ENGAGEMENT TYPE
Vulnerability Assessment + Gap Analysis

FRAMEWORKS
NIST CSF 2.0 · CIS Controls v8.1 (IG1)

REPORT DATE
Sample — illustrative only

CLASSIFICATION
Sample / Public

SAMPLE DELIVERABLE — NOT A REAL ENGAGEMENT

This is a demonstration document. The Village of Cedar Hollow is a fictional municipality created solely to illustrate Blue Line Cyber's assessment methodology and reporting style. All findings, systems, and evidence shown are invented for illustrative purposes and do not describe any real organization.

Blue Line Cyber LLC · Chicago, Illinois · bluelinecyber.io

SAMPLE

SECTION 1

Executive Summary

Blue Line Cyber conducted a vulnerability assessment and compliance gap analysis of the Village of Cedar Hollow's public-facing systems and core IT environment. This summary is written for Village leadership; technical detail follows in later sections.

Overall posture

Cedar Hollow has functional IT operations but lacks several foundational security controls that are now considered essential cyber hygiene. The most urgent issues are an outdated public website with known vulnerabilities and the absence of multi-factor authentication on administrative and email accounts. Both are routinely exploited in attacks against small municipalities. None of the issues identified require large expenditures to resolve — most are configuration and process changes achievable within 90 days.

Findings at a glance

1	2	3	2	1
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

Top three priorities

PRIORITY	ISSUE	WHY IT MATTERS
1	Outdated website CMS with known vulnerabilities (F-01)	Publicly exploitable; a common entry point for defacement and ransomware.
2	No multi-factor authentication on admin & email (F-02)	A single stolen password grants full access. MFA blocks the vast majority of account attacks.
3	Email domain can be spoofed — weak DMARC (F-03)	Attackers can send email that appears to come from the Village, enabling fraud against residents and staff.

Bottom line for leadership: Cedar Hollow's exposure is typical for a village its size and is fixable with modest, mostly no-cost effort. Prioritizing the three items above would meaningfully reduce the risk of a disruptive incident. Blue Line Cyber recommends a 90-day remediation plan (Section 5) and a validation re-test to confirm the fixes.

Essential cyber hygiene (CIS IG1) status

Assessed against the 56 safeguards that make up CIS Controls v8.1 Implementation Group 1 — the emerging minimum standard for any organization — Cedar Hollow currently meets an estimated **48%**. Reaching a strong baseline is realistic within one to two quarters.

SAMPLE

SECTION 2

Scope & Methodology

In scope

- Public-facing Village website and content management system
- Online utility (water) billing portal
- Village email domain and authentication configuration
- Externally reachable services and TLS/certificate posture
- Interview-based review of backup, incident response, and training practices

Out of scope

- Denial-of-service / stress testing
- Social engineering or phishing of staff
- Physical security
- Any system not explicitly authorized in the engagement's Rules of Engagement

Approach

The assessment followed Blue Line Cyber's standard methodology: **Identify → Assess → Analyze → Report**. Testing was non-destructive and conducted only against authorized, in-scope assets under signed authorization. Findings are mapped to CIS Controls v8.1 safeguards and rolled up to NIST CSF 2.0 functions for executive reporting.

PHASE	ACTIVITY	FRAMEWORK ANCHOR
Identify	Asset & service discovery, data sensitivity mapping	CSF Identify · CIS 1–3
Assess	Configuration, patch, email, and TLS review	CSF Protect/Detect · CIS 4–9
Analyze	Gap analysis vs. CIS IG1; severity scoring	CSF Identify
Report	Prioritized findings + remediation roadmap	CSF Govern

How to read severity

SEVERITY	MEANING
CRITICAL	Exploitable now with severe impact. Fix immediately.
HIGH	Significant risk. Fix within 30 days.
MEDIUM	Moderate risk. Fix within 90 days.
LOW	Minor risk. Address as resources allow.
INFO	No direct risk; hardening opportunity.

SECTION 3

Detailed Findings

F-01 Outdated website CMS with known vulnerabilities

CRITICAL

WHAT WE FOUND

The Village website runs a content management system several major versions behind current, with at least two plugins that have publicly documented, exploitable vulnerabilities. Version information is exposed publicly, making the site easy to fingerprint and target.

WHY IT MATTERS

Publicly known vulnerabilities in outdated CMS software are one of the most common ways small-government websites are compromised — leading to defacement, malware hosting, or a foothold for ransomware. Automated tools scan for exactly this.

EVIDENCE

```
# HTTP response header (illustrative)
X-Generator: CMS 7.82  <-- current stable is 10.x
# Two plugins flagged against public advisory database
plugin-a 2.4.1  [known RCE advisory]
plugin-b 1.9.0  [known XSS advisory]
```

RECOMMENDATION

Update the CMS core and all plugins to current supported versions on a scheduled basis. Remove unused plugins. Suppress version disclosure in response headers. Establish a recurring patch cadence (see F-05).

CIS Control: 7 — Continuous Vulnerability Management **CSF Function:** Protect / Identify **Effort:** Medium

F-02 No multi-factor authentication on administrative & email accounts

HIGH

WHAT WE FOUND

Administrative access to the website, the billing portal, and staff email accounts is protected by password only. No second factor is required.

WHY IT MATTERS

Passwords are routinely stolen through phishing and credential reuse. Without MFA, one stolen password gives an attacker full access. MFA blocks the overwhelming majority of account-takeover attempts and is often a requirement for cyber-insurance coverage.

RECOMMENDATION

Enable MFA on all administrative accounts, the email platform, and remote access — prioritizing any account with elevated privileges. Prefer app-based or hardware authenticators over SMS where available.

CIS Control: 6 — Access Control Management **CSF Function:** Protect **Effort:** Low

F-03 Email domain can be spoofed — weak DMARC policy

HIGH

WHAT WE FOUND

The Village domain publishes an SPF record but has no enforced DMARC policy (set to *none*), and DKIM is not consistently applied.

WHY IT MATTERS

Without an enforced DMARC policy, attackers can send emails that appear to come from an official Village address — a common tactic for invoice fraud, resident phishing, and impersonation of Village officials.

EVIDENCE

```
# DNS TXT lookup (illustrative)
_dmarc  "v=DMARC1; p=none"   <-- not enforced
spf     "v=spf1 include:_spf... ~all"  ok
dkim    not consistently present
```

RECOMMENDATION

Deploy DKIM across all sending sources, then move DMARC from *p=none* to *p=quarantine* and ultimately *p=reject* after monitoring. Review aggregate DMARC reports before enforcing.

CIS Control: 9 — Email & Web Browser Protections **CSF Function:** Protect **Effort:** Low

F-04 Weak TLS configuration on public services

MEDIUM

WHAT WE FOUND

Public web services permit legacy TLS 1.0/1.1 protocols and several weak cipher suites. HTTP Strict Transport Security (HSTS) is not enabled.

WHY IT MATTERS

Legacy protocols and weak ciphers can allow traffic interception under certain conditions and signal to auditors that the site is not maintained to current standards. Increasingly flagged by cyber-insurance assessments.

RECOMMENDATION

Disable TLS 1.0/1.1, restrict to strong cipher suites, and enable HSTS. Most hosting platforms allow this in a few configuration changes.

CIS Control: 4 — Secure Configuration **CSF Function:** Protect **Effort:** Low

F-05 No documented incident response plan

MEDIUM

WHAT WE FOUND

The Village has no written incident response plan. Staff could not point to a documented procedure for who to call, what to do, or how to communicate during a cyber incident.

WHY IT MATTERS

When an incident happens, the first hours matter most. Without a plan, response is improvised, recovery is slower, and mistakes are more likely. A basic plan dramatically improves outcomes.

RECOMMENDATION

Adopt a concise incident response plan covering roles, contacts (internal, legal, law enforcement, insurer), containment steps, and communication. Review annually and after any incident.

CIS Control: 17 — Incident Response Management **CSF Function:** Respond **Effort:** Medium

F-06 Backups are not regularly tested

MEDIUM

WHAT WE FOUND

Backups are performed, but restores are not routinely tested, and it is unclear whether backups are isolated from the primary network.

WHY IT MATTERS

A backup that has never been test-restored may not work when needed. Modern ransomware specifically targets connected backups — nearly all attacks on state and local government attempt to compromise them.

RECOMMENDATION

Test restores on a regular schedule, keep at least one backup copy offline or otherwise isolated, and document recovery time objectives.

CIS Control: 11 — Data Recovery **CSF Function:** Recover **Effort:** Medium

F-07 Verbose server headers disclose software versions

LOW

WHAT WE FOUND

Web server responses reveal specific software and version numbers.

WHY IT MATTERS

Version disclosure helps attackers match known exploits to the Village's software with less effort. Low risk on its own, but easy to remove.

RECOMMENDATION

Suppress or genericize server and framework version headers.

CIS Control: 4 — Secure Configuration **CSF Function:** Protect **Effort:** Low

F-08 No security awareness training program

LOW

WHAT WE FOUND

Village staff have not received security awareness training in the past year, and there is no recurring program.

WHY IT MATTERS

Most incidents begin with a person — a clicked link or a reused password. Brief, regular training measurably reduces successful phishing.

RECOMMENDATION

Introduce short annual (ideally quarterly) awareness training. Free resources from CISA can seed the program at no cost.

CIS Control: 14 — Security Awareness & Skills Training **CSF Function:** Protect **Effort:** Low

F-09 Missing HTTP security headers

INFO

WHAT WE FOUND

The website does not set several recommended security headers (Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy).

WHY IT MATTERS

These headers add defense-in-depth against common web attacks. Their absence is not directly exploitable but is a missed hardening opportunity.

RECOMMENDATION

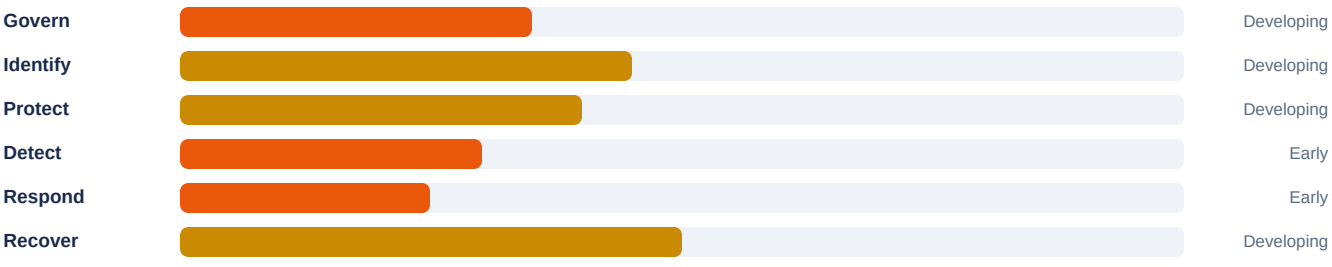
Add the recommended security headers at the web server or CDN layer.

CIS Control: 4 / 16 — Secure Config / App Security **CSF Function:** Protect **Effort:** Low

SECTION 4

Compliance Gap Summary

Findings rolled up to NIST CSF 2.0 functions. Bars show an approximate current maturity for each function based on this assessment.



Interpretation: Cedar Hollow's strongest area is basic recovery capability (backups exist), while **Respond** and **Detect** are the weakest — the Village would struggle to notice and react to an incident today. Closing the High findings (F-02, F-03) lifts **Protect** quickly; adopting an incident response plan (F-05) directly strengthens **Respond**.

SECTION 5

Remediation Roadmap

A prioritized, phased plan. Sequenced so the highest-impact, lowest-effort fixes come first.

Phase 1 — First 30 days (quick, high-impact)

FINDING	ACTION	EFFORT
F-02	Enable MFA on admin, email, and remote access	Low
F-03	Deploy DKIM; move DMARC to quarantine	Low
F-04	Disable legacy TLS; enable HSTS	Low
F-07	Suppress version disclosure headers	Low

Phase 2 — 30 to 60 days

FINDING	ACTION	EFFORT
F-01	Update CMS core & plugins; remove unused plugins	Medium
F-06	Test backup restores; isolate a backup copy	Medium
F-09	Add recommended HTTP security headers	Low

Phase 3 — 60 to 90 days (process & people)

FINDING	ACTION	EFFORT
F-05	Adopt and socialize an incident response plan	Medium
F-08	Launch recurring security awareness training	Low
—	Establish a standing patch cadence to prevent recurrence of F-01	Low

> **Projected outcome:** Completing all three phases would move Cedar Hollow from an estimated 48% to roughly 85% of CIS IG1 essential cyber hygiene, and materially strengthen every NIST CSF function — particularly Protect and Respond. Blue Line Cyber recommends a validation re-test at the end of the 90-day window to confirm fixes and document the improvement.

How Blue Line Cyber can help

- **Remediation support retainer** — hands-on help implementing the roadmap
- **Validation re-test** — confirm fixes and produce a before/after record
- **Ongoing advisory** — quarterly check-ins to maintain the baseline as the environment changes