COMPLIANCE LAYER

# example.com
# Security Assessment Report

| | |
|---|---|
| REPORT ID | CL-SR0FWDSN |
| TARGET DOMAIN | example.com |
| ASSESSMENT DATE | 2026-08-06 |
| OVERALL GRADE | B (87/100) |
| RISK LEVEL | LOW-MEDIUM |
| SCAN DURATION | 30679ms |
| TOTAL ISSUES | 23 |

OVERALL SCORE

Prepared for: sample@compliancelayer.net

Scan to check the assessment record
Scope: see Verification & Integrity

# Executive Summary

### Assessment Overview for example.com

The infrastructure scan evaluated 14 of 15 security modules and identified 23 total issues.
0 critical and 2 high-severity findings require immediate remediation.
The weakest area is Security Headers, scoring 60/100 (Grade C).
Strongest module: Blacklists at 100/100 (Grade A).
Not assessed this scan: Privacy & Trackers.

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 0 | 2 | 2 | 2 | 17 |

Issue Distribution

## Priority Recommendations

1. Add header: Strict-Transport-Security: max-age=31536000; includeSubDomains
2. Add header: Content-Security-Policy: default-src 'self'

# Module Scores

| MODULE | DESCRIPTION | SCORE | GRADE | WEIGHT | STATUS |
|---|---|---|---|---|---|
| Blacklists | IP & domain reputation lists | 100 | A | 0% | Pass |
| Breach Monitor | Known data breaches | 100 | A | 0% | Pass |
| Cookie Security | Cookie flags & attributes | 100 | A | 6% | Pass |
| DNS & Email Auth | SPF, DKIM, DMARC | 90 | A | 20% | Review |
| DNSSEC | DNS integrity & signing | 90 | A | 4% | Review |
| Security Headers | HTTP response headers | 60 | C | 25% | Action Needed |
| JavaScript | Client-side libraries | 100 | A | 2% | Pass |
| Port Security | Open port exposure | 100 | A | 15% | Pass |
| Reputation | Threat intelligence feeds | 100 | A | 0% | Pass |
| SSL/TLS | Certificate & encryption | 100 | A | 25% | Pass |
| Subdomains | Public certificate-record discovery | 100 | A | 0% | Pass |
| Technology | Tech stack detection | 100 | A | 0% | Pass |
| Privacy & Trackers | Third-party tracking | — | | — | Not Assessed |
| WAF Detection | Web application firewall | 100 | A | 3% | Pass |
| WHOIS | Domain registration | 100 | A | 0% | Pass |

Modules weighted 0% are informational: they are assessed and reported but do not affect the overall score.

# Module Analysis

## Security Headers HTTP response headers

60 /100 C

- Missing Strict-Transport-Security (HSTS) header
- Missing Content-Security-Policy (CSP) header
- Missing X-Frame-Options header

+1 more finding(s) in the Security Findings section

## DNS & Email Auth SPF, DKIM, DMARC

90 /100 A

- DMARC has no aggregate reporting address (rua)

## DNSSEC DNS integrity & signing

90 /100 A

- No CAA records found

## Blacklists IP & domain reputation lists

100 /100 A

- Domain and IP are clean on all 11 conclusively checked blacklists *Informational — not scored*

## Breach Monitor Known data breaches

100 /100 A

- No known data breaches associated with this domain *Informational — not scored*

## Cookie Security Cookie flags & attributes

100 /100 A

- No cookies set on initial page load *Informational — not scored*

**JavaScript** Client-side libraries

- No detectable JavaScript libraries with known patterns *Informational — not scored*

**100** /100 **A**

**Port Security** Open port exposure

**100** /100 **A**

**Reputation** Threat intelligence feeds

- VirusTotal: Clean (91 engines checked, 0 detections) *Informational — not scored*

**100** /100 **A**

**SSL/TLS** Certificate & encryption

**100** /100 **A**

**Subdomains** Public certificate-record discovery

- 2 subdomains found in public Certificate Transparency logs and public DNS datasets... *Informational — not scored*

**100** /100 **A**

**Technology** Tech stack detection

- Using CDN: Cloudflare *Informational — not scored*

**100** /100 **A**

**WAF Detection** Web application firewall

- WAF detected: Cloudflare (confidence: 100%) *Informational — not scored*

**100** /100 **A**

**WHOIS** Domain registration

- WHOIS registrant details are publicly visible (typical for corporate domains) *Informational — not scored*

**100** /100 **A**

### Privacy & Trackers

Not Assessed

This module did not produce a verdict.

# Security Findings

## HIGH (2)

### Missing Content-Security-Policy (CSP) header

Recommendation: Add header: Content-Security-Policy: default-src 'self'

### Missing Strict-Transport-Security (HSTS) header

Recommendation: Add header: Strict-Transport-Security: max-age=31536000; includeSubDomains

## MEDIUM (2)

### DMARC has no aggregate reporting address (rua)

Recommendation: Add rua=mailto:dmarc-reports@yourdomain.com to receive reports

### No CAA records found

Recommendation: Add CAA records to specify which Certificate Authorities can issue certificates for your domain. ...

## LOW (2)

### Missing X-Content-Type-Options header

Recommendation: Add header: X-Content-Type-Options: nosniff

**Missing X-Frame-Options header**

Recommendation: Add header: X-Frame-Options: DENY or SAMEORIGIN

## INFORMATIONAL — NOT SCORED (17)

**2 subdomains found in public Certificate Transparency logs and public DNS datasets. Cer...**

Recommendation: Audit the inventory periodically and retire unused hosts.

**DNSSEC is properly configured using ECDSAP256SHA256**

Recommendation: DNSSEC is protecting your domain from DNS spoofing.

**Domain and IP are clean on all 11 conclusively checked blacklists**

Recommendation: No action needed. Continue monitoring regularly.

**Domain has good reputation (score: 100/100) - verified by Google Safe Browsing and Viru...**

Recommendation: Continue maintaining good security practices.

**Missing Permissions-Policy header**

Recommendation: Add header: Permissions-Policy: geolocation=(), microphone=()

**Missing Referrer-Policy header**

Recommendation: Add header: Referrer-Policy: strict-origin-when-cross-origin

**Missing X-XSS-Protection header**

Recommendation: Add header: X-XSS-Protection: 1; mode=block (note: deprecated in modern browsers, use CSP instead)

**No cookies set on initial page load**

Recommendation: This is normal for static sites. Cookies may be set after authentication.

**No detectable JavaScript libraries with known patterns**

Recommendation: Site may use bundled/minified code. Consider additional auditing tools.

**No known data breaches associated with this domain**

Recommendation: Continue monitoring. Consider breach monitoring services.

**No sensitive subdomains identified among 2 discovered**

Recommendation: Good hygiene. Continue monitoring for new subdomains.

**No trackers detected in static HTML. This scan does not execute JavaScript; trackers lo...**

Recommendation: For comprehensive privacy auditing, use tools that execute the page (e.g. Blacklight, Ghostery, o...

**Technologies detected: Cloudflare, Cloudflare**

Recommendation: Regular security updates for all technologies are recommended.

**Using CDN: Cloudflare**

Recommendation: CDN provides performance and security benefits.

**VirusTotal: Clean (91 engines checked, 0 detections)**

Recommendation: Domain has good reputation.

**WAF detected: Cloudflare (confidence: 100%)**

Recommendation: WAF provides protection against common web attacks.

**WHOIS registrant details are publicly visible (typical for corporate domains)**

Recommendation: No action required. Individual registrants may prefer to enable WHOIS privacy.

# Compliance-Relevant Technical Controls

## SOC 2 Type II

**43%**
control coverage

Pass: 2/7 Partial: 2/7 Fail: 3/7

7 of 33 framework controls externally testable
6 further controls (MFA, backups, logging, incident response) require internal review

## PCI DSS 4.0.1

**31%**
control coverage

Pass: 2/8 Partial: 1/8 Fail: 5/8

8 controls externally testable
29 further controls (MFA, backups, logging, incident response) require internal review

## HIPAA Security Rule

**50%**
control coverage

Pass: 3/6 Partial: 0/6 Fail: 3/6

6 controls externally testable
18 further controls (MFA, backups, logging, incident response) require internal review

## NIST CSF 2.0

**20%**
control coverage

Pass: 1/5 Partial: 0/5 Fail: 4/5

5 of 106 framework controls externally testable
19 further controls (MFA, backups, logging, incident response) require internal review

## ISO 27001:2022

**31%**
control coverage

Pass: 2/8 Partial: 1/8 Fail: 5/8

8 of 93 framework controls externally testable
18 further controls (MFA, backups, logging, incident response) require internal review

## CIS Controls v8

**31%**
control coverage

Pass: 2/8 Partial: 1/8 Fail: 5/8

8 of 153 framework controls externally testable
20 further controls (MFA, backups, logging, incident response) require internal review

**Compliance record digest: 799A-9913-3115-7D69** - compare with the value shown at the verification URL on the cover.

# Assessed Controls

Control identifiers are authoritative; names are our summaries. Look up wording in the standard using the identifier.

### SOC 2 Type II

| | | |
|---|---|---|
| **CC6.6** | FAIL | Security measures against threats |
| **CC6.7** | FAIL | Restrict transmission/movement of data |
| **CC6.8** | FAIL | Prevent/detect unauthorized software |
| **CC6.1** | PARTIAL | Logical and Physical Access Controls |
| **CC9.1** | PARTIAL | Business continuity objectives |
| **CC7.1** | PASS | Detect configuration changes |
| **CC7.2** | PASS | Monitor system components |

### PCI DSS 4.0.1

| | | |
|---|---|---|
| **1.2.1** | FAIL | Restrict connections |
| **11.6.1** | FAIL | Change/tamper detection mechanisms |
| **2.2.4** | FAIL | Configure system security parameters |
| **4.2.1** | FAIL | Strong cryptography |
| **6.2.4** | FAIL | Software engineering techniques prevent cross-site scripting |
| **5.4.1** | PARTIAL | Mechanisms detect and protect personnel against phishing attacks |
| **1.3.1** | PASS | Restrict inbound traffic |
| **2.2.5** | PASS | Enable only necessary services |

### HIPAA Security Rule

| | | |
|---|---|---|
| **164.308(a)(5)(ii)(B)** | FAIL | Protection from malicious software |
| **164.312(c)(1)** | FAIL | Integrity |
| **164.312(e)(1)** | FAIL | Transmission Security |
| **164.308(a)(1)(ii)(D)** | PASS | Information system activity review |
| **164.312(a)(1)** | PASS | Access Control |
| **164.312(e)(2)(ii)** | PASS | Encryption |

### NIST CSF 2.0

| | | |
|---|---|---|
| **PR.DS-01** | FAIL | The confidentiality, integrity, and availability of data-at-rest are protected |
| **PR.DS-02** | FAIL | The confidentiality, integrity, and availability of data-in-transit are protected |
| **PR.IR-01** | FAIL | Networks and environments are protected from unauthorized logical access and usage |
| **PR.PS-01** | FAIL | Configuration management practices are established and applied |
| **ID.RA-01** | PASS | Vulnerabilities in assets are identified, validated, and recorded |

## ISO 27001:2022

| | | |
|---|---|---|
| **A.8.20** | **FAIL** | Networks security |
| **A.8.26** | **FAIL** | Application security requirements |
| **A.8.27** | **FAIL** | Secure system architecture and engineering principles |
| **A.8.7** | **FAIL** | Protection against malware |
| **A.8.8** | **FAIL** | Management of technical vulnerabilities |
| **A.5.14** | **PARTIAL** | Information transfer |
| **A.8.15** | **PASS** | Logging |
| **A.8.24** | **PASS** | Use of cryptography |

## CIS Controls v8

| | | |
|---|---|---|
| **12.2** | **FAIL** | Secure network architecture |
| **16.1** | **FAIL** | Secure application development process |
| **16.11** | **FAIL** | Use standard hardening configuration |
| **3.10** | **FAIL** | Encrypt sensitive data in transit |
| **4.1** | **FAIL** | Establish secure configuration process |
| **9.5** | **PARTIAL** | Implement DMARC |
| **13.1** | **PASS** | Network monitoring and defense |
| **9.2** | **PASS** | Use DNS filtering services |

# About This Report

## Assessment Methodology

This report was generated by the ComplianceLayer Infrastructure Risk Intelligence platform.
The assessment performs non-intrusive external scanning across 15 security modules:
8 carry scoring weight proportional to underwriting materiality, and 7 are
informational (assessed and reported, but not scored).

Modules: Blacklists, Breach Monitor, Cookie Security, DNS & Email Auth, DNSSEC, JavaScript, Port Security, Privacy & Trackers, Reputation, SSL/TLS, Security Headers, Subdomains, Technology, WAF Detection, WHOIS.

Compliance mapping covers SOC 2 Type II, PCI DSS 4.0.1, HIPAA Security Rule, NIST CSF 2.0, ISO 27001:2022, CIS Controls v8.

## Important Caveats & Limitations

- This score assesses externally observable technical controls only. It does not evaluate internal security, policies, procedures, or organizational maturity.
- A high score indicates strong external hygiene but does not guarantee insurability. Other factors include claims history, industry sector, revenue, data handling practices, and incident response capabilities.
- A low score indicates technical gaps that should be remediated, but does not automatically disqualify coverage. Underwriters will assess compensating controls and risk appetite.
- External scans cannot detect internal threats such as insider risk, weak passwords, unpatched endpoints, lack of MFA, or inadequate backups. These are assessed separately.
- This is a point-in-time assessment. Security posture changes over time. Continuous monitoring is recommended for maintained visibility.
- Some checks may produce false negatives (e.g., DKIM with custom selectors). Manually verify configurations with service providers when applicable.

## Grading Scale

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A | 90-100 Low Risk | B | 75-89 Low-Medium Risk | C | 55-74 Medium Risk | D | 35-54 High Risk | F | 0-34 Critical Risk |

## Severity Levels

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| Immediate action | Urgent fix needed | Should address soon | Minor improvement | Informational only |

## Verification & Integrity

**Verification URL: https://compliancelayer.net/verify/CL-SR0FWDSN**
**Compliance record digest: 799A-9913-3115-7D69**

**What verification confirms:**

- The report file as a whole. The SHA-256 digest shown at the verification URL is taken over the complete document, so the compliance table and every finding in it are covered by that one value even though their contents are not repeated on the page.
- The target domain, assessment date, overall score and grade, risk level, issue counts and module scores, read from the record created when the scan ran.
- Whether this assessment is still current, or has been superseded by a corrected scan engine.

**What verification does NOT confirm:**

- Any file whose digest does not match. ComplianceLayer cannot attest to a document it did not serve: compute this file's SHA-256 digest and compare it with the one shown at the verification URL.
- A report the verification page reports as not attested. Those were issued before document binding existed and cannot be proven retroactively, because no record was kept of what was emitted.
- Anything added by a reseller or intermediary after the report was issued, including white-label branding.
- Whether the organisation is compliant. This is an external technical assessment, not a certification.