Passive IT Risk Report

example.com

Report date: 1/7/2026

Overall Risk Score

72
/100
Moderate

Legend: Green (Low) • Orange (Moderate) • Red (High)

What Moderate means

This score indicates increased exposure to common web-based attacks. No breach detected yet — however, current gaps significantly increase the likelihood of abuse before detection.

Industry benchmark

Financial Services average: 85 / E-commerce average: 78 / Your score: 72 (below industry average)

Benchmarks are indicative and based on aggregated public posture observations.

Interpretation: Organizations below industry average are more likely to receive audit observations and executive scrutiny.

At a glance

Top risks identified:

DMARC policy is missing

HIGH

No DMARC record was found for the domain.

Evidence: **No TXT record found for _dmarc.example.com**

Business impact: **Invoice fraud and brand impersonation risk increases without DMARC enforcement.**

HTTP is not redirected to HTTPS

HIGH

Requests over HTTP are not forced to HTTPS for the same host.

Evidence: **GET http://example.com -> 200 without redirect**

Business impact: **Users may stay on insecure HTTP, enabling interception or tampering.**

Content Security Policy is missing

MEDIUM

No CSP header was found on the homepage response.

Evidence: **No Content-Security-Policy header detected.**

Business impact: **Increases exposure to XSS and data exfiltration in the browser.**

Generated by CyberFaceX Passive IT Risk Intelligence - cyberfacex.com
Report ID: sample-6c44d26b
Generated at: 1/7/2026 | Integrity hash: SHA256 45ea9ac25a62bf96

Executive Summary

Designed for executive review and audit preparation.

What this means for your business

Email spoofing, missing web security headers, and weak TLS hygiene increase the risk of invoice fraud, browser-based attacks, and data interception.

- Increased likelihood of invoice fraud
- Higher exposure to browser-based attacks
- Elevated risk during TLS renewal periods

Top risks

DMARC policy is missing

HIGH

No DMARC record was found for the domain.

Evidence: **No TXT record found for _dmarc.example.com**
Business impact: **Invoice fraud and brand impersonation risk increases without DMARC enforcement.**

HTTP is not redirected to HTTPS

HIGH

Requests over HTTP are not forced to HTTPS for the same host.

Evidence: **GET http://example.com -> 200 without redirect**
Business impact: **Users may stay on insecure HTTP, enabling interception or tampering.**

Content Security Policy is missing

MEDIUM

No CSP header was found on the homepage response.

Evidence: **No Content-Security-Policy header detected.**
Business impact: **Increases exposure to XSS and data exfiltration in the browser.**

30-day action plan

Addressing P0 and P1 items within 30 days will significantly reduce your overall risk score.

P0	Publish DMARC with p=quarantine/reject; align SPF/DKIM	Prevent invoice fraud and spoofing
P1	Enforce HTTPS and enable HSTS (preload-ready)	Prevent downgrade and session hijacking
P1	Add CSP, X-Frame-Options, Referrer-Policy	Reduce XSS, clickjacking, data leakage
P2	Automate TLS renewal and monitor expiry	Reduce outage and trust erosion
P2	Track owners and deadlines for remediation	Ensure fixes land within 30 days

Execution risk: Without ownership tracking and verification, most remediation plans fail within 60 days.

Executive decision matrix

Risk	Fix cost	Impact	Priority
DMARC policy is missing	Low	High	Fix now
HTTP is not redirected to HTTPS	Low	High	Fix now
Content Security Policy is missing	Low	Medium	Plan

Generated by CyberFaceX Passive IT Risk Intelligence - cyberfacex.com
Report ID: sample-6c44d26b
Generated at: 1/7/2026 | Integrity hash: SHA256 45ea9ac25a62bf96

Risk Score Breakdown

Email Security 60

Acceptable

Transport Security 75

Acceptable

Web Security 70

Acceptable

Redirect & Hygiene 65

Acceptable

Audit readiness score

Audit readiness score is a governance indicator, not a certification.

56 / 100 (At risk)

Scores below 75 typically result in audit observations.

Top risks with evidence

DMARC policy is missing

HIGH

No DMARC record was found for the domain.

Evidence: **No TXT record found for _dmarc.example.com**
Business impact: **Invoice fraud and brand impersonation risk increases without DMARC enforcement.**

HTTP is not redirected to HTTPS

HIGH

Requests over HTTP are not forced to HTTPS for the same host.

Evidence: **GET http://example.com -> 200 without redirect**
Business impact: **Users may stay on insecure HTTP, enabling interception or tampering.**

Content Security Policy is missing

MEDIUM

No CSP header was found on the homepage response.

Evidence: **No Content-Security-Policy header detected.**
Business impact: **Increases exposure to XSS and data exfiltration in the browser.**

Findings Overview

Severity	Finding	Category	Evidence
! HIGH	DMARC policy is missing	email_security	No TXT record found for _dmarc.example.com
! HIGH	HTTP is not redirected to HTTPS	hygiene	GET http://example.com -> 200 without redirect
~ MEDIUM	Content Security Policy is missing	web_security	No Content-Security-Policy header detected.
~ MEDIUM	TLS certificate expires soon	transport_security	Certificate expires in 9 days
~ MEDIUM	HSTS header is missing	transport_security	No Strict-Transport-Security header detected.
- LOW	X-Frame-Options is missing	web_security	No X-Frame-Options header detected.

Compliance mapping

This report helps identify gaps against common security frameworks.

HSTS missing	PCI DSS 4.0 (A.6), OWASP ASVS
HTTPS not enforced	ISO 27001 A.13
DMARC missing/p=none	Email Security Best Practices

Audit exposure

- ISO 27001: Likely audit observation
- PCI DSS: Control gap (non-compliant)
- Internal audit: High-risk finding

Generated by CyberFaceX Passive IT Risk Intelligence - cyberfacex.com
Report ID: sample-6c44d26b
Generated at: 1/7/2026 | Integrity hash: SHA256 45ea9ac25a62bf96

Detailed Findings

DMARC policy is missing

HIGH

No DMARC record was found for the domain.

What we observed

No TXT record found for _dmarc.example.com

Business impact

Invoice fraud and brand impersonation risk increases without DMARC enforcement.

Risk escalation timeline

- 0–30 days: Increased abuse attempts
- 30–90 days: Likely misuse or audit finding
- 90+ days: High probability of financial or reputational incident

Recommended actions

- Publish DMARC with p=quarantine or p=reject
- Align SPF and DKIM before enforcing

Estimated effort: High | Owner: Email / IT

HTTP is not redirected to HTTPS

HIGH

Requests over HTTP are not forced to HTTPS for the same host.

What we observed

GET http://example.com -> 200 without redirect

Business impact

Users may stay on insecure HTTP, enabling interception or tampering.

Risk escalation timeline

- 0–30 days: Increased abuse attempts
- 30–90 days: Likely misuse or audit finding
- 90+ days: High probability of financial or reputational incident

Recommended actions

- Add a 301 redirect from HTTP to HTTPS
- Enable HSTS preload after testing redirects

Estimated effort: High | Owner: IT

Content Security Policy is missing

MEDIUM

No CSP header was found on the homepage response.

What we observed

No Content-Security-Policy header detected.

Business impact

Increases exposure to XSS and data exfiltration in the browser.

Recommended actions

- Define a restrictive CSP for scripts/styles/connect sources
- Roll out with report-only first, then enforce

Estimated effort: Medium | Owner: Web / IT

TLS certificate expires soon

MEDIUM

The certificate validity ends within 14 days.

What we observed

Certificate expires in 9 days

Business impact

Risk of service disruption and user trust loss if renewal is missed.

Recommended actions

- Renew the TLS certificate
- Automate certificate renewal (e.g., ACME)

Estimated effort: Medium | Owner: IT

HSTS header is missing

MEDIUM

Strict-Transport-Security is not set, so browsers may downgrade to HTTP.

What we observed

No Strict-Transport-Security header detected.

Business impact

Opens opportunity for SSL stripping and downgrade attacks.

Recommended actions

- Add HSTS with long max-age and includeSubDomains
- Consider preload after validating redirects

Estimated effort: Medium | Owner: IT

X-Frame-Options is missing

LOW

The response does not prevent clickjacking via iframes.

What we observed

No X-Frame-Options header detected.

Business impact

Attackers could frame your site to trick users into unintended actions.

Recommended actions

- Set X-Frame-Options: DENY or SAMEORIGIN

Estimated effort: Low | Owner: Web / IT

Generated by CyberFaceX Passive IT Risk Intelligence - cyberfacex.com
Report ID: sample-6c44d26b
Generated at: 1/7/2026 | Integrity hash: SHA256 45ea9ac25a62bf96

Methodology

- Passive-only signals: DNS, TLS handshake, HTTP response headers, redirect checks.
- No port scanning, no authentication, no intrusive probes.
- Findings reflect best-practice configuration from public signals.

Passive analysis only — no intrusive scanning performed.

Trust note
This report is based solely on publicly observable signals and does not require authorization.

Generated by CyberFaceX Passive IT Risk Intelligence - cyberfacex.com
Report ID: sample-6c44d26b
Generated at: 1/7/2026 | Integrity hash: SHA256 45ea9ac25a62bf96