SF SaaSFort

NIS2 Compliance Assessment

EU Directive 2022/2555 — Article 21(2) Technical Measures

GENERATED	COMPLIANCE DEADLINE	READINESS	DOMAINS ASSESSED
4 June 2026	17 October 2026	In Progress	1

Compliance Overview

80%	6	2	1	1
OVERALL	COMPLIANT	PARTIAL	NON-COMPLIANT	NOT ASSESSED

91 total checks performed · 73 passed · 18 failed across 10 NIS2 Art.21(2) controls

Assessed Domains

DOMAIN	GRADE	SCORE	SCANNED
saasfort.com	B	85/100	4 Jun 2026 06:02 UTC

Article 21(2) Control Assessment

NIS2 Art.21(2)(a) — Governance

COMPLIANT

Risk analysis & information system security policies

100%

6 checks performed · 6 passed · 0 failed

NIS2 Art.21(2)(b) — Incident Response

COMPLIANT

Incident handling & vulnerability disclosure

100%

2 checks performed · 2 passed · 0 failed

NIS2 Art.21(2)(c) — Resilience

Business continuity & crisis management

NOT ASSESSED

0%

0 checks performed · 0 passed · 0 failed

No automated checks mapped. Manual assessment required.

NIS2 Art.21(2)(d) — Supply Chain

Supply chain security

COMPLIANT

100%

2 checks performed · 2 passed · 0 failed

NIS2 Art.21(2)(e) — Network Security

Network & information system security

COMPLIANT

90%

21 checks performed · 19 passed · 2 failed

LOW — DNSSEC
DNSSEC not enabled — DNS responses can be spoofed without detection

LOW — COOP enforcement level
Cross-Origin-Opener-Policy not set — browsing context can be accessed by cross-origin popups

NIS2 Art.21(2)(f) — Vulnerability Mgmt

Vulnerability handling & management

PARTIAL

85%

14 checks performed · 12 passed · 2 failed

MEDIUM — Admin panel exposure
Admin path /admin returns 200 — may expose admin interface

LOW — Rate limiting
No rate limiting detected — consider implementing for brute-force prevention

Address 2 failing checks.

NIS2 Art.21(2)(g) — Cyber Hygiene

NON-COMPLIANT

Cybersecurity hygiene & training

38%

18 checks performed · 7 passed · 11 failed

MEDIUM — CSP
Missing Content-Security-Policy header — Prevents XSS and code injection attacks

MEDIUM — Clickjacking protection
Missing X-Frame-Options header — Prevents your site from being embedded in iframes

LOW — MIME sniffing protection
Missing X-Content-Type-Options header — Prevents browsers from MIME-type sniffing

LOW — Referrer policy
Missing Referrer-Policy header — Controls referrer information leakage

LOW — Permissions policy
Missing Permissions-Policy header — Restricts browser features (camera, geolocation, etc.)

LOW — Server header
Server software disclosed — helps attackers fingerprint your stack

MEDIUM — Clickjacking protection
Neither X-Frame-Options nor CSP frame-ancestors present — site can be embedded in malicious iframes

LOW — Robots.txt sensitive paths
robots.txt reveals sensitive paths — attackers use this for reconnaissance

LOW — Technology fingerprint
Technology detected: Astro, Svelte — attackers can target known vulnerabilities

LOW — X-Download-Options
X-Download-Options header not set — IE users may be able to open downloads in site context

LOW — COOP enforcement level
Cross-Origin-Opener-Policy not set — browsing context can be accessed by cross-origin popups

Critical: 11 of 18 checks failing.

NIS2 Art.21(2)(h) — Cryptography

COMPLIANT

Cryptography & encryption policies

95%

21 checks performed · 20 passed · 1 failed

LOW — OCSP stapling
OCSP stapling not detected — revocation checking may add latency for clients

NIS2 Art.21(2)(i) — Access Control

PARTIAL

Access control & asset management

50%

4 checks performed · 2 passed · 2 failed

MEDIUM — Admin panel exposure
Admin path /admin returns 200 — may expose admin interface

LOW — Rate limiting
No rate limiting detected — consider implementing for brute-force prevention

Address 2 failing checks.

NIS2 Art.21(2)(j) — Authentication

COMPLIANT

Multi-factor authentication & secure communications

100%

3 checks performed · 3 passed · 0 failed