

NIS2 Art. 21(2)(d) & DORA Art. 28 Supplier Posture Handbook

Quantitative Third-Party Domain, Email Anti-Spoofing & Transport Cryptography Governance for UK & EU Entities

Section 1: Why Static Vendor Questionnaires Fail Regulator Audits

Under **EU NIS2 Directive Article 21(2)(d)**, **EU DORA Article 28 (ICT Third-Party Risk Management)**, **ISO/IEC 27001:2022 Annex A.5.19–A.5.22**, and the **UK Cyber Security and Resilience Bill (2026)**, essential and important entities must verify the technical cybersecurity posture of their direct ICT, legal, payroll, and logistics suppliers.

Over 73% of supply-chain financial fraud begins with **Vendor Email Compromise (VEC)** or **Direct Domain Spoofing** of a trusted supplier's invoicing domain. A vendor that ticks "Yes" on a self-assessment questionnaire while running `v=DMARC1; p=none` or an broken 12-lookup SPF record remains completely spoofable.

Section 2: Quantitative 100-Point Supplier Scoring Rubric

CONTROL DOMAIN	MAX POINTS	PASS / PARTIAL CRITERIA	REGULATORY CLAUSE MAPPING
1. DMARC Enforcement & Telemetry	35 pts	<code>p=reject</code> + <code>rua=</code> (35 pts) • <code>p=quarantine</code> (26 pts) • <code>p=none</code> (8 pts) • Missing (0 pts)	NIS2 Art. 21(2)(d) & (j) • DORA Art. 28(8) • ISO 27001 A.5.20
2. SPF Strictness & RFC 7208 Lookups	20 pts	<code>-all</code> & ≤ 10 lookups (20 pts) • <code>~all</code> & ≤ 10 lookups (12 pts) • > 10 lookups <code>permxrror</code> (4 pts)	NIS2 Art. 21(2)(d) • DORA Art. 9(2) • RFC 7208 Sec 4.6.4
3. MTA-STS & SMTP TLS-RPT	15 pts	<code>_mta-sts</code> + <code>_smtp._tls</code> active (15 pts) • MTA-STS only (10 pts) • TLS-RPT only (5 pts)	NIS2 Art. 21(2)(h) Cryptography • DORA Art. 9(3) Transit
4. CAA Certificate Lock	10 pts	Explicit <code>issue</code> / <code>issuewild</code> CAA record present (10 pts) • Missing (0 pts)	NIS2 Art. 21(2)(h) • ISO 27001 A.8.24
5. HTTPS HSTS Header	10 pts	<code>Strict-Transport-Security</code> header enforced on HTTPS root (10 pts)	DORA Art. 9(3) • UK CE v3.3 Sec A1.1
6. RFC 9116 security.txt	10 pts	<code>/.well-known/security.txt</code> returns HTTP 200 with <code>Contact:</code> (10 pts)	NIS2 Art. 21(2)(e) Vulnerability Handling • DORA Art. 17

Section 3: Running Bulk Supplier Audits (`nis2\_supplier\_auditor.py`)

The included Python 3 CLI auditor (`scripts/nis2\_supplier\_auditor.py`) requires zero third-party packages and queries live Cloudflare/Google DNS-over-HTTPS (DoH) plus HTTPS headers.

3.1 Auditing a Vendor Portfolio File (`--domains-file`)

Populate `templates/Supplier-Domains-Sample.txt` with one supplier per line (either plain domain names or CSV rows with `domain,Criticality_Tier,Service_Category`):

```
meridian-cloud-uk.co.uk,Tier 1 (Critical ICT),Cloud Hosting & Payroll
apex-managed-it.co.uk,Tier 1 (Critical ICT),Managed Service Provider (MSP)
sterling-legal-llp.co.uk,Tier 2 (Important),External Legal & M&A Counsel
```

Then execute the auditor to produce your Board HTML Report and DORA Register of Information (RoI) CSV:

```
python3 scripts/nis2_supplier_auditor.py --domains-file templates/Supplier-Domains-Sample.txt -
-output-dir ./audit-q4
```

3.2 Diagnosing the RFC 7208 SPF 10-Lookup `permerror` Trap

Many SaaS-heavy suppliers chain multiple `include:` statements in their SPF record (``spf.protection.outlook.com`,`_spf.google.com`,`sendgrid.net`,`mailgun.org`,`hubspot.com``). Under **RFC 7208 Section 4.6.4**, once total DNS-querying mechanisms (``include`,`a`,`mx`,`ptr`,`exists`,`redirect``) exceed **10 lookups**, receiving mail gateways return `SPF permerror`—causing legitimate supplier emails to fail authentication or forcing the supplier to leave DMARC at `p=none`.

Remediation Guidance for Suppliers Exceeding 10 SPF Lookups: Instruct the vendor to move bulk marketing/transactional senders (SendGrid, HubSpot, Mailchimp) onto dedicated subdomains (``mail.supplier.co.uk`` or ``billing.supplier.co.uk``) so the root corporate domain (``@supplier.co.uk``) stays at ≤ 4 DNS lookups with strict `-all` termination.

Section 4: 30-Day Vendor Remediation SLA & Escalation Playbook

When a Tier 1 or Tier 2 supplier scores below **70/100 (Grade C, D, or F)**, follow this four-stage governance workflow:

SUPPLIER SCORE	ACTION CLASSIFICATION	MANDATORY GOVERNANCE & PAYMENT VERIFICATION CONTROL
80–100 (A / A+)	COMPLIANT	Log HTML & CSV evidence in annual NIS2/DORA Supply-Chain Register. Re-audit semi-annually.
70–79 (B)	ADVISORY SENT	Send courtesy hardening advisory recommending MTA-STS, TLS-RPT, and `security.txt` within 90 days.
35–69 (C / D)	30-DAY NOTICE REQUIRED	Issue formal <code>Supplier-Remediation-Notice-Email.md</code> requiring progression from `p=none` to `p=quarantine`/`p=reject` within 30 days.
0–34 (F)	CRITICAL SPOOFING RISK	Immediate Accounts Payable Hold on Email Bank Changes: Enforce out-of-band voice verification for any invoice/IBAN update from this vendor until DMARC is enforced.

4.1 Copy-Paste DNS Records to Provide to Non-Compliant Suppliers

```
; 1. Staged DMARC Enforcement Record (_dmarc.supplier.co.uk)
_dmarc.supplier.co.uk. 3600 IN TXT "v=DMARC1; p=quarantine; pct=100;
rua=mailto:dmarc@supplier.co.uk; adkim=r; aspf=r;"

; 2. Strict Microsoft 365 SPF Record (supplier.co.uk)
supplier.co.uk. 3600 IN TXT "v=spf1 include:spf.protection.outlook.com -all"

; 3. SMTP MTA-STS & TLS-RPT Records
_mta-sts.supplier.co.uk. 3600 IN TXT "v=STSV1; id=20261025;"
_smtp_tls.supplier.co.uk. 3600 IN TXT "v=TLSRPTv1; rua=mailto:tls-rpt@supplier.co.uk"
```

Section 5: External Auditor Evidence Checklist (NIS2 / DORA / ISO 27001)

Present the following four artifacts during your ISO/IEC 27001:2022 surveillance audit, DORA Register of Information (RoI) filing, or Competent Authority inspection:

ITEM	REGULATORY REQUIREMENT	VERIFICATION ARTIFACT	RETENTION CADENCE
☐ 01	NIS2 Art. 21(2)(d) Supply-Chain Risk Register	NIS2-DORA-Supplier-Register.csv (UTF-8 BOM spreadsheet)	Quarterly Snapshot
☐ 02	DORA Art. 28 Executive Oversight Evidence	NIS2-DORA-Executive-Board-Report.html (Signed PDF/HTML)	Quarterly Board Pack
☐ 03	ISO 27001:2022 A.5.21–A.5.22 Supplier Monitoring	NIS2-DORA-ISO27001-Control-Crosswalk.csv	Annual Statement of Applicability
☐ 04	Vendor Deficiency Tracking & 30-Day SLA Notices	Sent copies of Supplier-Remediation-Notice-Email.md	Per Non-Compliant Vendor

Interactive 5-Domain Browser Scanner: Need to run an instant ad-hoc check during a procurement call? Use our 100% Free Forever browser batch scanner at <https://faultypacket.co.uk/nis2-dora-supplier-posture-auditor.html>.