DNS Compliance & Governance Framework

A Continuous DNS Posture Management Program

Version 1.0 | July 2026 | **Applicable frameworks:** SOC 2, ISO 27001:2022, NIS2 Directive, DORA, PCI-DSS v4.0

Executive Summary

DNS is a critical but frequently overlooked security and compliance control surface. Misconfigurations, dangling records, and unauthorized changes can lead to subdomain takeovers, email spoofing, certificate fraud, and regulatory findings.

This framework establishes a **continuous DNS posture management program** that helps organizations maintain real-time visibility, address requirements across multiple regulatory frameworks, reduce risk, and gather audit evidence efficiently rather than through last-minute manual effort.

Important: This framework is provided for informational and planning purposes. The control mappings reflect common interpretations of how DNS relates to each framework and are **not a substitute for guidance from a qualified auditor or compliance advisor**, who should confirm how these controls apply to your specific environment and obligations.

1. Purpose and Scope

This document defines minimum recommended practices for managing DNS as a critical security and compliance asset.

In scope: All external and internal domains, subdomains, delegated zones, and DNS infrastructure, including third-party DNS providers.

2. Roles and Responsibilities

Role	Key Responsibilities	Review Frequency
CISO / Security Leadership	Overall risk ownership, policy approval, executive reporting	Quarterly
DNS / Infrastructure Team	Configuration, changes, zone maintenance	Ongoing
Security / GRC Team	Compliance mapping, evidence collection, risk assessments	Monthly
IT / DevOps	Application DNS usage and record requests	As needed
Third-Party Risk Management	Oversight of external DNS providers	Quarterly
Incident Response Team	DNS-related incident handling	As needed

3. Control Checklist with Recommended Frequencies

3.1 DNS Asset Inventory & Discovery

Control	Frequency	Implementation Notes	Evidence
Registered domain inventory	Quarterly + continuous	Registrar APIs and WHOIS data	Master domain register
Subdomain discovery	Monthly + ad-hoc	Continuous discovery (e.g. via Certificate Transparency)	Subdomain inventory export
Shadow IT & forgotten domains	Quarterly	Cross-reference with marketing, dev, and other teams	Shadow domain report

3.2 DNS Security Controls

Control	Frequency	Implementation Notes	Evidence
CAA records	Initial + Quarterly	Restrict certificate issuance to authorized CAs	CAA validation export
DNSSEC	Ongoing + Annual testing	Documented key rollover procedures	DNSSEC status records
Dangling records	Monthly	Automated detection + remediation	Change history / remediation log
Wildcard records	Quarterly	Minimize and scope usage	Wildcard inventory export

3.3 Email Authentication

- SPF, DKIM, and DMARC configured and reviewed – **Quarterly**
- DMARC aggregate report monitoring – **Weekly**

3.4 Change Management & Auditing

- All changes logged and approved through your change process – **Every change**
- Real-time detection and alerting on unauthorized or unexpected changes – **Real-time**
- Change-history retention – **12 to 24 months**

> Note on tooling: a monitoring layer such as DNS Assistant **detects and alerts on** changes and maintains a viewable change history. Change **approval** is enforced within your own workflow; the monitoring layer provides the detection and evidence around it.

3.5 Continuous Monitoring & Alerting

- Monitor new and removed records, expirations, and anomalies – **Real-time**
- Route alerts to SIEM and ticketing (via API and webhooks) – **Ongoing**

3.6 Third-Party & Supply-Chain DNS

- DNS provider inventory and risk assessment – **Quarterly**
- Monitor third-party delegations for unexpected change – **Ongoing**

3.7 Disaster Recovery

- Multi-provider DNS for critical domains – **Ongoing**
- Failover testing – **Annually**
- Zone file backups – **Monthly**

3.8 Incident Response (DNS-Specific)

- Define DNS incident categories and response procedures – **As needed + annual exercise**

3.9 Documentation, Reporting & Metrics

- Posture review and evidence export – **Monthly**
- Governance review – **Quarterly**

4. Risk Scoring Matrix

Risk Level	Score	Description	Target Remediation SLA
Critical	5	Immediate high impact (e.g. active takeover exposure)	< 4 hours
High	4	Significant risk requiring prompt action	< 7 days
Medium	3	Moderate risk	< 30 days
Low	2	Minor risk	< 90 days

5. Standards Mapping (Summary)

Framework	Representative DNS-Relevant Controls
SOC 2	CC6.1, CC7.2 – change monitoring and logical access
ISO 27001:2022	A.5.9, A.8.1, A.8.32 – asset management and change control
NIS2	Article 21 – supply-chain and risk management
DORA	ICT third-party risk and incident reporting
PCI-DSS v4.0	Requirements 1, 2, 3, 4 – secure configuration and transmission

> The mappings above are illustrative and non-exhaustive. Confirm applicability and completeness with your auditor or compliance advisor.

Appendix A: Glossary

Term	Definition
Dangling record	A DNS record pointing to a resource that no longer exists, creating takeover risk
DNSSEC	DNS Security Extensions; cryptographic authentication of DNS data
CAA record	Certification Authority Authorization; controls which CAs may issue certificates
DMARC	Domain-based Message Authentication, Reporting and Conformance
Shadow DNS	DNS records or subdomains created outside central governance