NIS2 & DORA Cybersecurity Gap Check

Do you have provable control over email, domains, and DNS?

Governance & Accountability:

Can management prove cyber risk is under control?

	Yes	No	Partial
Executives understand cyber risk and their accountability	☐	☐	☐
Clear ownership of email, domain, and DNS security	☐	☐	☐
Audit-ready reporting available for regulators	☐	☐	☐

Email Security (Inbound):

Are phishing attacks stopped before users see them?

Phishing and malware blocked before inbox delivery	☐	☐	☐
Email security does not rely only on user awareness	☐	☐	☐
Evidence of blocked threats available for audits	☐	☐	☐
Native M365/Google security validated against real threats	☐	☐	☐

Domain & Outbound Email:

Can attackers send email in your name?

DMARC enforced (quarantine/reject), not p=none	☐	☐	☐
All domains protected (primary, parked, defensive)	☐	☐	☐
Domain spoofing actively blocked	☐	☐	☐
Clear ownership and evidence of domain controls	☐	☐	☐

DNS Availability & Resilience:

Would a DNS failure become a reportable incident?

DNS infrastructure is globally resilient (Anycast)	☐	☐	☐
DNS decoupled from application hosting	☐	☐	☐
DNS changes are governed and auditable	☐	☐	☐
DNS costs are predictable and fixed	☐	☐	☐

Detection & Evidence:

Can you prove prevention, not just response?

Prevented incidents visible in real time	☐	☐	☐
Evidence preserved for audits and reporting	☐	☐	☐
Management-level reporting in place	☐	☐	☐

Scoring & Next Steps

All "Yes"
Largely aligned with NIS2 & DORA

Some "Partial"
Review and strengthen weak areas

Red: Any "No"
Urgent gaps requiring immediate action

Next Steps

1. Identify where risk still reaches users, inboxes, or services
2. Close enforcement gaps across email, domains, and DNS
3. Establish clear ownership and audit-ready evidence
4. Demonstrate board-level due care under NIS2 and DORA

Contact us:
We'll help you understand where exposure typically exists and how Avanan, ECP, and Enterprise DNS map directly to NIS2 and DORA expectations.

abion