CFO REFERENCE GUIDE

# NIS2 for Growing Companies:

## What CFOs Need to Know

## A practical reference for finance leaders at EU and EEA companies

# What NIS2 Is and Why It's Different

NIS2 — the Network and Information Security Directive 2 — is a mandatory EU cybersecurity regulation that came into force across EU member states in October 2024. It is not a certification you pursue when a customer asks. It is a legal obligation with regulatory supervision and significant penalties for non-compliance.

NIS2 replaced its predecessor (NIS1) and dramatically expanded scope — both in terms of which sectors are covered and which companies within those sectors must comply.

## Three things make NIS2 different from ISO 27001 or SOC 2:

### It is mandatory

Not a competitive differentiator but a **legal floor**.

### No certificate at the end

Compliance is demonstrated through **documented controls, incident reporting, and regulatory supervision**.

### Personal accountability

Senior management is explicitly held **personally accountable** — NIS2 is one of the few cybersecurity frameworks that can result in personal liability for directors and executives.

fortifai

# NIS2 and Norway — What EEA Companies Need to Know

NIS2 is an EU directive. Norway is not an EU member state but is part of the European Economic Area (EEA), which means EU internal market legislation — including cybersecurity directives — applies to Norway through the EEA agreement.

NIS2 will be incorporated into Norwegian law via the EEA process. The transposition timeline for EEA countries runs slightly behind EU member states, but the direction is clear and the obligations are the same. Norwegian companies in covered sectors should treat NIS2 as an active compliance obligation and not wait for formal national transposition before beginning gap assessments.

Additionally, Norwegian companies that supply EU-based essential or important entities are already subject to NIS2 requirements through their customers' supply chain obligations — regardless of when Norway formally transposes the directive into national law.

**The practical advice:** treat NIS2 as in force for your compliance planning now. The cost of early preparation is far lower than the cost of being caught in a regulatory gap.

fortifai

# Who NIS2 Applies To

NIS2 covers two categories — and the threshold is lower than most companies expect:

| Category | Sectors | Size Threshold |
|---|---|---|
| **Essential Entities** | Energy, transport, banking, financial market infrastructure, health, water, digital infrastructure, ICT service management, public administration, space | 250+ employees or €50M+ turnover |
| **Important Entities** | Postal and courier, waste management, chemicals, food, manufacturing, digital providers (online marketplaces, search engines), research | 50+ employees or €10M+ turnover |

### Supply chain pull-in

Even if your company falls below these thresholds, if you are a critical supplier to an essential or important entity, that entity's NIS2 obligations flow through to your contracts. Procurement teams at large European companies are already adding NIS2 compliance requirements to vendor agreements.

### If you are unsure whether NIS2 applies

Conduct a scope determination before assuming it doesn't. The cost of an unnecessary gap assessment is far lower than the cost of a regulatory investigation.

fortifai

# What NIS2 Requires From You as CFO

NIS2 explicitly places accountability at management level — not the IT department. Article 20 of the directive states that management bodies must approve cybersecurity risk management measures, oversee their implementation, and can be held personally liable for infringements.

These are the approvals and actions NIS2 requires from executive leadership:

| What You're Signing or Owning | When | What a Regulator Checks |
|---|---|---|
| Cybersecurity Risk Management Policy | Before compliance deadline, reviewed annually | Board-level approval documented, policy current |
| Risk Assessment and Treatment Decisions | Before controls implemented, reviewed annually | Documented assessment with named executive sign-off |
| Supply Chain Security Policy | Before compliance deadline | Vendor inventory, assessment records, contract clauses |
| Business Continuity and Crisis Management Plan | Before compliance deadline | Documented, approved, tested |
| Incident Reporting Decision | Within 24 hours of significant incident | Named decision-maker, documented assessment of significance |
| Management Oversight of Controls | Ongoing | Evidence of board-level review — minutes, decisions, actions |
| Annual Cybersecurity Training | Annually | Completion records for management and board members |

**The 24-hour incident reporting obligation is the highest-risk area for most CFOs.** NIS2 requires an initial notification to your national competent authority within 24 hours of becoming aware of a significant incident — before you necessarily understand its full scope. Finance leaders own the materiality assessment: is this incident significant enough to trigger reporting? The decision must be documented and defensible. Having a pre-agreed decision framework before an incident occurs is not optional — it is the difference between a managed notification and a regulatory finding.

# High-Level Compliance Checklist

**1**

### Scope and Gap Assessment

- Confirm whether your company is an essential or important entity
- Identify which national competent authority supervises your sector
- Appoint a named NIS2 compliance owner — with board-level executive sponsor
- Complete gap assessment against NIS2 Article 21 requirements
- Review supplier contracts for NIS2 flow-down obligations
- Register with national authority if required by your member state
- For Norwegian companies: monitor EEA transposition timeline and assess supply chain obligations from EU customers now

**2**

### Risk Assessment

- Complete cybersecurity risk assessment covering all in-scope systems
- Document threat landscape, vulnerabilities, likelihood, and impact
- CFO signs off on risk treatment decisions
- Document residual risk acceptance with named executive owner
- Schedule annual risk assessment review

**3**

### Policy Documentation

- Draft and approve: Cybersecurity Risk Management Policy, Incident Handling Policy, Business Continuity Policy, Supply Chain Security Policy, Access Control Policy, Encryption Policy, Vulnerability Management Policy
- Board or management body formally approves all policies
- Publish to all relevant staff with acknowledgment records
- Set annual review dates for each policy

**4**

### Control Implementation

- Access controls — MFA, least privilege, joiner/mover/leaver process
- Network security — segmentation, monitoring, logging with retention
- Vulnerability management — scanning schedule, patch process, penetration test
- Encryption — data at rest and in transit, key management documented
- Supply chain assessments — questionnaires sent to key suppliers, responses documented
- Business continuity — backup verification, recovery test, results documented
- Incident response — playbooks documented, tabletop exercise completed

**5**

### Incident Reporting Framework

- Define what constitutes a "significant incident" for your organisation
- Document the decision framework — who decides, on what criteria, within what timeframe
- Identify your national competent authority and document contact details
- Establish 24-hour notification procedure with named decision-maker
- Establish 72-hour detailed report procedure
- Test the process — run a simulated incident notification exercise

**6**

### Ongoing Compliance

- Annual risk assessment review and CFO sign-off
- Annual policy reviews with board approval
- Annual cybersecurity training for management and board — completion records maintained
- Supply chain reassessments on contract renewal cycle
- Management review of control effectiveness — documented outputs
- Monitor NIS2 transposition updates if operating in Norway or other EEA states

# Manual vs. Automated: What Good Looks Like

| NIS2 Requires | Manual Reality | With Governance Automation |
|---|---|---|
| Board-approved risk management policy | Approved once, stored in shared drive, never updated | Version-controlled, annual review triggered automatically |
| 24-hour incident reporting decision | No pre-agreed framework, decision made under pressure | Pre-built decision framework with notification workflow ready |
| Supply chain security assessments | Sent once, filed and forgotten | Recurring workflow tied to contract renewal dates |
| Management oversight evidence | Meeting happened, no documented output | Structured review with timestamped sign-off and action log |
| Annual training completion records | Spreadsheet, incomplete, hard to produce | Automated tracking with retrievable completion records |

NIS2 has no annual certification audit — but regulators can request evidence of compliance at any time, and significant incidents will trigger supervisory scrutiny. The organisations that handle that scrutiny well are the ones that treat compliance as a **continuous operating discipline**, not an annual project.

fortifai

# What the Penalties Look Like

This is the section most CFOs read first — and rightly so.

## €10M

### Essential Entities

€10 million or 2% of global annual turnover — whichever is higher

## €7M

### Important Entities

€7 million or 1.4% of global annual turnover — whichever is higher

### Personal liability for senior management is explicitly included

Member states must enable competent authorities to hold natural persons in management positions personally liable for NIS2 infringements — including temporary bans from management roles for serious or repeated violations.

### For Norwegian companies

EEA transposition will carry equivalent enforcement provisions. Additionally, Norwegian companies already subject to NIS2 obligations through their customers' supply chains face contractual liability and potential commercial consequences independent of regulatory enforcement.

This is the provision that elevates NIS2 from an IT compliance task to a board governance matter — and the reason the sign-off trail matters as much as the controls themselves.

fortifai

# How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing companies. The platform automates the three workflows NIS2 requires: sign-off routing and tracking for board-level policy approvals, disclosure document management for incident reporting and regulatory submissions, and information request handling for supply chain assessments and regulatory evidence requests — pre-configured for NIS2 with templates ready on day one.

The same platform supports ISO 27001, SOC 2, GDPR, and other frameworks simultaneously. For companies managing multiple compliance obligations, the governance workflows overlap significantly and the evidence base is shared — so adding NIS2 to an existing ISO 27001 or GDPR programme is materially less work than starting from scratch.

### Sign-off Routing

Automated tracking for board-level policy approvals with timestamped records

### Disclosure Management

Incident reporting and regulatory submissions with pre-built notification workflows

### Information Requests

Supply chain assessments and regulatory evidence requests handled in one place

Fortifai is used by teams at **Cognite, Aker BioMarine, and Telenor.**

> **Book a 30-minute walkthrough at [fortifai.co](fortifai.co)**

fortifai