Move2Cloud

• WHITE PAPER — 2027 EDITION

CYBERSECURITY & COMPLIANCE

NIS2
Achieving Compliance Before the Deadline

The practical guide for French SMEs and mid-caps: who is in scope, what the directive really requires, and how to structure compliance without mobilising a dedicated team.

11 pages · Self-assessment checklist, transposition timeline and roadmap included

15,000
French entities affected, versus around 500 under NIS1

€10M
maximum fine for an essential entity in case of non-compliance

2%
of global annual turnover, a possible alternative to the fixed fine

PREPARED BY
Move2Cloud — Cloud & Infrastructure Consulting, Paris

PUBLICATION
September 2026

CONTENTS

What you will find in this document

A six-step journey, from the question "am I in scope?" to an operational compliance roadmap.

01 **Executive summary — the essentials on one page** p.3

02 **Why NIS2 changes everything for SMEs and mid-caps** p.4

03 **Am I in scope? Sectors, thresholds, categories** p.5

04 **What NIS2 actually requires** p.6

05 **Penalties and executive liability** p.7

06 **Where France stands: transposition timeline** p.8

07 **Self-assessment grid** p.9

08 **A 5-step roadmap** p.10

09 **Conclusion & about Move2Cloud** p.11

Who is this document for? Executives, CIOs and CISOs of SMEs and mid-caps who are discovering, or suspect, that they fall under NIS2 and are looking for a clear method to objectively assess their situation.

Copyright Move2Cloud — move2cloud.fr

EXECUTIVE SUMMARY

The essentials on one page

NIS2 is no longer reserved for large groups and operators of vital importance — it redefines the perimeter of regulated cybersecurity in France, and sweeps in thousands of SMEs and mid-caps that were not expecting it.

The European NIS2 directive (2022/2555) considerably broadens the scope of the previous 2016 NIS directive. In France, its transposition takes the form of the law on the resilience of critical infrastructure and the strengthening of cybersecurity, known as the "resilience law", still under parliamentary review even though the country has passed the initial European deadline of 17 October 2024. The concrete result: **around 15,000 French entities will be concerned**, compared with roughly 500 under the former NIS1 regime — a perimeter multiplied by thirty.

This extension covers 18 sectors of activity, split across two levels of criticality, and two categories of entities with differentiated obligations. The penalties, for their part, are calibrated to deter: **up to 10 million euros or 2% of worldwide turnover** for an essential entity in breach, with liability that can reach all the way up to the executives themselves.

For an SME or mid-cap that has never had to comply with a sector-specific cyber regulation, the first question is not "how do I become compliant?" but "am I genuinely in scope, and under which category?". This document sets out a method for answering it, before detailing the concrete obligations that follow.

15,000
French entities concerned, versus around 500 under NIS1 — a 30x wider perimeter

18
sectors of activity covered, split across two levels of criticality

€10M
maximum fine for an essential entity, or 2% of worldwide turnover

For an SME or mid-cap that has never had to comply with a sector-specific cyber regulation, the first question is not "how do I become compliant?" but "am I genuinely in scope, and under which category?". This document sets out a method for answering it, before detailing the concrete obligations that follow.

SECTION 02

Why NIS2 changes everything for SMEs and mid-caps

The 2016 NIS directive covered only a limited number of operators deemed critical — essentially large groups in energy, transport or healthcare. Experience showed that this approach left out a growing share of the digital value chains on which those same critical sectors depend.

1. The scope extends across the entire dependency chain

NIS2 is no longer limited to large operators: it now covers their suppliers, subcontractors and digital service providers as soon as they exceed certain size thresholds. An IT services SME or a mid-cap industrial firm can thus find itself in scope simply because it supplies a service to an entity that is itself subject to the directive.

2. Size thresholds replace individual designation

Unlike NIS1, where each Member State individually designated the operators concerned, NIS2 relies on objective headcount and turnover thresholds, applied sector by sector. This automation of the scope largely explains the shift from 500 to 15,000 entities in France.

3. Governance accountability becomes explicit

NIS2 introduces a requirement that did not exist under NIS1: the direct involvement of management bodies in cyber risk management, with liability that can be incurred personally in the event of a serious and repeated breach.

> *“ NIS2 does not ask you to be invulnerable — it asks you to demonstrate that cyber risk is managed as a business risk. ”*

For any organisation supplying services to a client subject to NIS2 — even without being directly caught by the thresholds — compliance also becomes a commercial question, since that client must ensure its critical providers comply too.

Copyright Move2Cloud — move2cloud.fr

SECTION 03

Am I in scope? Sectors, thresholds, categories

Three combined criteria determine whether NIS2 applies: the sector of activity, the size of the entity, and the resulting level of criticality.

SCOPE CRITERION	WHAT IT COVERS
Highly critical sectors (Annex I)	Energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, space.
Essential entity (EE)	≥250 employees, or turnover >€50M and balance sheet >€43M, in Annex I sectors: full obligations, proactive supervision by the national authority, the highest penalties.
Important entity (IE)	≥50 employees, or turnover >€10M, across Annexes I and II; any large Annex II company: similar obligations, but reactive supervision (ex-post control) and penalties capped at a lower level.

Key takeaway: An SME with fewer than 50 employees may still be in scope if it is the only identified critical supplier of an essential entity, or if a Member State has designated it individually — the thresholds are the general rule, not an absolute guarantee of exclusion.

18 sectors, two levels of criticality

The directive distinguishes "highly critical" sectors (Annex I) from "critical" sectors (Annex II), with similar obligations but a different supervision regime. Annex II covers postal services, waste management, chemical substances, food production, manufacturing (several industrial sub-sectors), digital providers and research — which means a company can be fully in scope without ever having considered itself a critical operator.

Copyright Move2Cloud — move2cloud.fr

SECTION 04

What NIS2 actually requires

Beyond the broad principles, NIS2 lists precise risk-management measures that every entity in scope must be able to demonstrate.

DOMAIN	KEY FIGURE	WHAT IS EXPECTED	PRIORITY FOR
Incident management	24h / 72h	A procedure for detecting, handling and notifying significant incidents, with an early warning to the competent authority within 24 hours and a detailed report within 72 hours.	Organisations with no formalised detection chain
Risk analysis	Reviewed regularly	A documented policy for risk analysis and information system security, reviewed on a regular basis.	Every entity in scope, as the baseline documentation
Business continuity	Tested backups	A continuity and disaster recovery plan, including crisis management and the management of tested backups.	Entities whose outage would affect critical clients

Common pitfall: The 24-hour notification deadline for an early warning is particularly demanding for an organisation that does not yet have a formalised detection procedure — it is often the first workstream to launch, even before the full risk analysis.

Supply chain, cyber hygiene and governance

Three further domains complete the picture. Supply chain security requires the security of direct suppliers and service providers to be assessed and built into contractual relationships. Cyber hygiene and training cover access control policies, encryption, multi-factor authentication and regular awareness-raising across teams. Governance requires the direct involvement and training of management bodies in cyber risk management, with formal approval of the measures adopted.

Copyright Move2Cloud — move2cloud.fr

SECTION 05

Penalties and executive liability

NIS2 aligns the level of cyber penalties with that of the GDPR — a clear signal of the priority given to the directive at European level.

Measures that go beyond the fine

Beyond fines, essential entities face suspension of certifications and the liability of their executives, while important entities are exposed to administrative injunctions and periodic penalty payments.

Liability that reaches up to the board

Management bodies can now be held personally liable for serious and repeated breaches of risk-management obligations — shifting cybersecurity from a purely technical topic to one of corporate governance.

Support first, penalties later

National authorities will initially favour a supportive approach over immediate sanction for good-faith entities engaged in a compliance process — but this tolerance is neither permanent nor guaranteed.

ENTITY CATEGORY	FAILURE TO MANAGE RISKS OR TO NOTIFY
Essential entity	Up to €10M or 2% of global turnover, plus possible suspension of certifications and executive liability.
Important entity	Up to €7M or 1.4% of global turnover, plus administrative injunctions and periodic penalty payments.

Copyright Move2Cloud — move2cloud.fr

SECTION 06

Where France stands: transposition timeline

France has missed the original European transposition deadline, but the legislative process is actively continuing.

A single text for NIS2, CER and DORA

The transposition of NIS2 into French law takes the form of a bill on the resilience of critical infrastructure and the strengthening of cybersecurity — a text that simultaneously transposes NIS2 and the CER directive (resilience of critical entities), and dovetails with the DORA regulation for the financial sector. Having missed the 17 October 2024 deadline set by the European directive, France is subject to an infringement procedure opened by the European Commission — a situation shared with several other Member States.

What is already under way

Registration of the entities concerned is carried out through a dedicated platform, and transitional support is planned before penalties come fully into force — generally in the order of several years after the implementing texts are published, to give entities time to become compliant.

> **Key takeaway:** The absence of a definitively enacted law is no excuse for not preparing. The substantive obligations of the European directive are known and stable; only the precise national implementation arrangements (registration timetable, supervisory authority, graduated penalties) remain to be finalised. Organisations waiting for enactment to start will begin with a backlog they will then have to clear under pressure.

This transition period is not a reason to postpone the work: the substantive measures (risk management, notification, continuity) themselves take several months to put in place properly.

Copyright Move2Cloud — move2cloud.fr

SECTION 07

Self-assessment grid

Before launching a compliance programme, check these points to get an objective view of your current situation.

- [ ] **Have you checked whether your sector appears in one of the directive's two annexes?** Sector scope is the first condition of applicability, even before the size of the entity.
- [ ] **Does your headcount or turnover exceed the thresholds applicable to your sector?** Thresholds differ between essential and important entities, and between Annex I and Annex II.
- [ ] **Are you a direct supplier to an entity that is itself subject to NIS2?** Being designated a critical supplier can bring you into scope even below the general thresholds.
- [ ] **Do you have a formalised incident detection and notification procedure?** The 24-hour deadline for the early warning is one of the most technically demanding obligations.
- [ ] **Is the security of your critical suppliers and service providers assessed and documented?** Supply chain security is an integral part of the NIS2 obligations.
- [ ] **Have your executives been trained on their responsibilities regarding cyber risk management?** Involvement of the governance bodies is an explicit requirement, not a mere recommendation.

> **How to read your answers:** Three "no" answers or more, particularly on the sector and threshold questions, justify a formal applicability assessment before any other decision — it is the unavoidable starting point of any NIS2 initiative.

Copyright Move2Cloud — move2cloud.fr

SECTION 08

A 5-step roadmap

A progressive approach, designed to turn a regulatory obligation into a structural improvement of the organisation's security.

1

Assess applicability

Determine precisely whether the organisation is in scope, under which category (essential or important), and on the basis of which criteria — sector, thresholds, or critical supplier status.

2

Map the existing setup

Take stock of the security measures already in place against the directive's requirements, in order to identify the gaps precisely rather than starting from scratch.

3

Prioritise by risk and lead time

Tackle first the most structuring obligations and those that take longest to put in place — incident notification, business continuity, supply chain security.

4

Involve governance

Train the governance bodies, formalise their involvement in approving the measures, and document this governance so that it stands up in the event of an inspection.

5

Test and document continuously

Put in place regular exercises (incident simulation, continuity testing) and keep a documented record of the approach, a prerequisite for any demonstrable compliance.

Copyright Move2Cloud — move2cloud.fr

CONCLUSION

NIS2, a constraint that can become an advantage

Organisations that approach NIS2 as a structural security project — rather than as a regulatory box to tick — come out of it with a more mature risk governance, a real commercial advantage with customers who are themselves subject to the directive, and an operational resilience that goes well beyond the scope of compliance.

Waiting for the final enactment of the French text before starting means underestimating the real time required by measures such as incident notification or business continuity — these are projects prepared in months, not in weeks.

Move2Cloud	is a consulting firm specialised in infrastructure, cloud and IT transformation. We support organisations in the audit, compliance and securing of their cloud environment.
Contact	Move2Cloud — Paris · move2cloud.fr
Next step	A NIS2 applicability assessment makes it possible to answer the seven questions on page 9 within a few weeks, together with a prioritised compliance plan.

Sources

Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2) — Legiscope — "Transposition NIS2 en France : loi, calendrier 2026 et obligations ANSSI" — AdevWeb — "NIS2 : votre PME est-elle concernée ? 18 secteurs, calendrier 2026, sanctions" — ANSSI documentation on the NIS2 directive

Document written by Move2Cloud as an example and illustration, for educational purposes. The French legislative calendar is evolving; the information reflects the state of transposition at the publication date and does not constitute legal advice.