unosecur

WHITEPAPER

NIS2, Cloud and Identity

A practical guide for essential and important entities

Table of contents

Executive summary

NIS2 is the EU's updated cybersecurity framework, expanding the scope of the original NIS Directive and setting higher, harmonised standards for cybersecurity governance, risk management, reporting, and oversight. In cloud and SaaS estates, identity is the operational control surface: every user, machine identity, and API token must be visible, governed, and provable.

This paper explains NIS2's core chapters through the lens of cloud and identity. We outline practical controls, timelines, and evidence your supervisory authority will expect, map key Articles to identity-centric operations, and close by showing how Unosecur helps entities demonstrate compliance, not just claim it.

Introduction

NIS2 strengthens EU-wide cybersecurity by expanding the number of covered entities, defining essential and important sectors, and setting higher expectations for governance, risk management, incident reporting, and supervision.

For cloud-heavy environments, the directive's expectations translate directly into identity hygiene, access governance, and evidence-quality telemetry. Over-privileged accounts, stale tokens, or unmonitored service accounts can undermine compliance across multiple Articles.

This guide explains each NIS2 chapter in clear, operational terms, with a focus on what cloud-first organizations should implement and what supervisors will look for.

Section 1: General Provisions (Articles 1-6)

Scope, classification, and definitions

NIS2 expands the original directive's scope and introduces the classification of essential and important entities (Article 3). Organisations must determine where they fall, understand sector-specific obligations, and document how proportionality is applied.

For cloud/SaaS estates, this means mapping which systems support essential services, which identities operate them, and how privilege, exposure, and dependencies factor into risk.

Section 2: Coordinated cybersecurity frameworks (Articles 7–13)

Strategies, CSIRTs, vulnerability disclosure, and cooperation

Member States must maintain national cybersecurity strategies, designate competent authorities, and establish CSIRTs with defined roles in incident handling. NIS2 formalises vulnerability disclosure (Article 12) and emphasises coordinated responses across entities and authorities.

In cloud environments, this requires reliable telemetry: identity anomalies, token misuse, and API abuse must be detectable and reportable to CSIRTs with minimal friction.

Section 3: Cooperation at Union and international level (Articles 14–19)

EU-level networks, reporting, and peer review

The Cooperation Group, CSIRTs Network, and EU-CyCLONe underpin the directive's collective resilience model. Essential and important entities should be able to produce metrics, incident summaries, and risk reports to support Member State peer-review processes under Article 19.

Cloud-first organisations must ensure that identity logs, access summaries, and anomaly detections can be exported in structured, anonymized formats that align with Union reporting schemes.

Section 4: Cybersecurity risk-management measures and reporting obligations (Articles 20–25)

Governance, supply-chain risk, and incident reporting

Articles 20–23 contain the operational backbone of NIS2. Entities must implement:

- Governance and risk ownership at the management level
- Access control, least privilege, and secure configurations
- Supply-chain risk assessments, including SaaS and cloud dependencies
- Mandatory incident reporting timelines (early warning, notification, and final report)

In cloud/SaaS environments, these obligations translate into:

- Continuous visibility of all identities, human and non-human
- Privilege minimization for users, workloads, and CI/CD systems
- Monitoring for misuse, elevation, or credential compromise
- Evidence-quality logs for 24-hour and 72-hour reporting

Section 5: Jurisdiction and registration (Articles 26–28)

Jurisdiction rules and entity registries

NIS2 sets criteria for determining jurisdiction and requires Member States to maintain up-to-date entity registries. These are administrative responsibilities; organisations must maintain accurate self-identification, but the technical burden is minimal.

Section 6: Information-sharing (Articles 29–30)

Voluntary exchange of threat intelligence

Entities are encouraged to join information-sharing arrangements and exchange anonymized threat data, patterns, and lessons learned.

Cloud-first organisations should be able to share sanitized access anomalies, privilege drift patterns, and identity misuse indicators without exposing user or customer data.

Section 7: Supervision and enforcement (Articles 31–37)

Audits, enforcement, and penalties

Supervisory authorities may conduct audits, request evidence, inspect access logs, and impose corrective measures or penalties.

Entities must be able to produce:

- Identity-access artifacts (privilege assignments, changes, approvals)
- Incident-handling files
- Logs showing prevention, detection, and timely response
- Evidence of least privilege enforcement

Least privilege becomes a provable control: supervisors increasingly expect to see reduced standing privileges, temporary elevation, and traceability of access decisions across cloud systems.

Section 8: Delegated and implementing acts (Articles 38–39)

Legal adaptations and execution

These Articles define how the Commission may adopt delegated or implementing acts. They do not impose operational responsibilities on entities beyond staying adaptable.

Section 9: Final provisions (Articles 40–46)

Review, amendments, and entry into force

Supervisors will expect measurable progress across audit cycles.

Cloud/SaaS estates should track:

- Reduction in stale or excessive entitlements
- Token- and credential-reuse detections
- Elevation duration and frequency
- Time taken to remove compromised identities
- Mean time to detect (MTTD) and respond (MTTR) to identity misuse

NIS2 is not a one-off compliance event — it requires ongoing maturity.

How Unosecur proves resilience under NIS2

Identity Fabric

One view of every human and non-human identity across AWS, Azure, GCP, Okta, Google Workspace, Salesforce, and more. Maps identities to systems supporting essential and important services, helping entities classify scope under Articles 2–3 and assess exposure and dependency risk.

Exports risk scores and access summaries directly into supervisory evidence packs.

IAM Ops and IAM Analyzer

Minimise standing privilege, enforce Just-in-Time and Just-Enough-Privilege for admin roles, and surface unused or excessive entitlements.

Every privilege grant, elevation, and policy change is logged immutably — giving supervisors a clear line-of-sight into whether least privilege is enforced across cloud and SaaS systems under Articles 20–23 and 31–33.

Identity Threat Detection and Response (ITDR)

Monitor every access transaction in near real time, flag anomalies such as token reuse, privilege jumps, suspicious API calls, or SSO bypass, and orchestrate workflowed responses.

Produces structured artefacts for early warning, notification, and final reports under NIS2's incident-reporting timelines.

Evidence and Reporting

Generate regulator-ready artefacts: access logs, attestation outcomes, incident files, vulnerability-handling evidence, supply-chain identity summaries, and long-term maturity metrics.

Outputs align naturally with Articles 10–12, 20–23, and 31–33, helping entities organise evidence for supervisory reviews and cooperation obligations.

Quick mapping table

NIS2 Chapter / Article	What the Regulation Requires	Cloud & Identity Interpretation
Section 1(1–6) General Provisions	Scope, entity classification, definitions	Map cloud/SaaS identities, systems, and dependencies to essential /important services; document proportionality
Chapter 2 (7–13) CSIRTs, national strategies, disclosure	Threat reporting, coordinated response, vulnerability handling	Detect identity threats, produce disclosure-ready artifacts from CI/CD and SaaS logs
Chapter 3 (14–19) EU-level cooperation	Network-level reporting, metrics, and peer review	Export anonymized identity risk metrics; provide cross-tenant patterns

Chapter 4 (20–25) Governance, risk management, supply-chain, reporting	Access controls, least privilege, supply-chain oversight, and incident reporting	Enforce JIT/JEP, govern SaaS identities, produce 24h/72h-ready evidence
Chapter 5 (26–28) Jurisdiction, registries	Administrative requirements	Maintain clean inventories of cloud/SaaS systems and accountable owners
Chapter 6 (29–30) Info-sharing	Threat intelligence exchange	Share sanitized identity-anomaly datasets and privilege-drift patterns
Chapter 7 (31–37) Supervision & enforcement	Audits, evidence, penalties, breach handling	Provide access logs, privilege trails, identity-breach reports, and least-privilege documentation
Chapter 8 (38–39) Delegated acts	Regulatory processes	Ensure flexibility for future standards
Chapter 9 (40–46) Final provisions	Review, amendments, entry into force	Maintain longitudinal metrics and identity maturity tracking

Conclusion

Operational resilience under NIS2 comes down to three fundamentals: see every identity, minimise privilege, and prove it on demand. NIS2 provides the structure; cloud and identity provide the leverage. Security is serious, but your evidence pack should be effortless, complete, and always ready for inspection.

Disclaimer

This paper is informational and not legal advice. Confirm interpretations with counsel and your competent authority.

Verification notes (for your records)

- **Transposition deadline:** 17 October 2024 (obligations apply through national implementing laws; enforcement dates vary by Member State).
- **Incident reporting timelines:** early warning within 24 hours of awareness; incident notification within 72 hours; final report within one month after notification (progress updates required where relevant).
- **Risk-management obligations:** continuous cybersecurity controls under Articles 20–21, including access control, incident handling, business continuity, vulnerability handling, and supply-chain security (including cloud and SaaS providers).
- **Supervision model:** proactive (ex-ante) supervision for essential entities; reactive (ex-post) supervision for important entities by national competent authorities.
- **EU-level coordination:** Cooperation Group, CSIRTs Network, and EU-CyCLONe (no Lead Overseer model under NIS2).

Trusted by security leaders

Unosecur's agentless onboarding approach helped us to strategize and streamline our cloud identity security efforts. The proof of value was achieved in no time, helping us to fix existing identity blind spots.

Vijay Muthu
CISO, Rakuten Symphony

Rakuten Symphony

Ready to secure your enterprise identities?

Speak to the Unosecur team for a unified identity assessment.

Book a demo

unosecur.com