EMA PETROVIĆ / PRACTICAL FIELD GUIDE / EP-01

NIS2 Management Brief

Five questions, an accountability map and a supplier-assurance checklist for leadership teams.

Preview edition v0.1

ENGLISH + SRPSKI / SEPTEMBER 2026

Ema Petrović

NIS2 Officer | Cybersecurity governance and cyber law

Independent point of view | Built from practice

MANAGEMENT LENS

Five questions before the control list

NIS2 becomes useful when leadership can connect decisions, accountability, suppliers and evidence.

01

What is truly in scope?

Critical services, processes, data, systems and dependencies.

02

Who decides and who oversees?

Decision rights, reporting, escalation and approval of measures.

03

What evidence shows the system works?

Not only policies, but decisions, tests, training and corrective action.

04

How do we govern supplier risk?

Criteria, contracts, evidence, monitoring and changes in risk.

05

How does an incident reach leadership?

Thresholds, rehearsed roles and decisions under time pressure.

ACCOUNTABILITY MAP

One system, several owners

No single function can implement NIS2 alone. Leadership connects decisions, resources and oversight.

FUNCTION	KEY DECISION	EXAMPLE EVIDENCE
Leadership	Approves measures, resources and risk acceptance.	Decisions, minutes, indicators and follow-up of corrective action.
Legal	Translates obligations into governance and contracts.	Obligations register, clauses, legal assessments.
Procurement	Builds cyber criteria into supplier selection and monitoring.	Due diligence, criteria, reviews and exceptions.
Cyber / IT	Designs, operates and tests controls.	Test results, logs, vulnerabilities and remediation plans.
Operations	Protects continuity of critical services.	BIA, continuity plans, exercises and lessons learned.
HR and process owners	Defines roles, access, training and behaviour.	Access matrices, training, role acknowledgements and offboarding.

A responsibility matrix is useful only when it is connected to real decisions, reporting thresholds and evidence.

SUPPLIER RISK

The contract is not the end of assurance

Allocating duties on paper does not remove the company's need to understand and oversee the dependency.

What to verify with a supplier

- ☐ Which legal entities, services, systems and locations are in scope?
- ☐ Who issued the evidence, and is the issuer competent and verifiable?
- ☐ How long is it valid, and how are material changes communicated?
- ☐ What incident notification and cooperation duties are contractual?
- ☐ What alternative arrangement exists if the supplier fails?

If a supplier cites ISO/IEC 27001

- ☐ Request a copy of the current certificate.
- ☐ Check the certification body and validity period.
- ☐ Read the scope: does it cover the actual service?
- ☐ Check covered locations and the certified legal entity.
- ☐ Record what the certificate does not prove for your use case.

A PRACTICE EXAMPLE

A healthcare supplier stated only that it held ISO/IEC 27001 certification. Without the scope, issuer and validity, the statement did not show that the certificate covered the service on which the company relied. Asking for evidence is not distrust. It is risk governance.

EVIDENCE AND ACTION

From documents to a visible system

Begin with a small evidence set that shows decision, implementation, testing and improvement.

EVIDENCE	OWNER	WHAT IT SHOULD SHOW
Management decision	Leadership	What was approved, on which information and under which conditions.
Risk register	Risk owner	Risk, treatment, deadline, status and acceptance of residual risk.
Supplier review	Procurement / security	Criticality, evidence requested, findings, exceptions and follow-up.
Test or exercise	IT / operations	Scenario, result, weakness, corrective-action owner and deadline.
Training and roles	HR / leadership	Who needs to know what, participation and evidence of understanding.

THE FIRST 30 DAYS

01 Days 1-7

Confirm scope, critical services and decision owners.

02 Days 8-14

Map current measures and evidence, not only policies.

03 Days 15-21

Tier suppliers by criticality and review major dependencies.

04 Days 22-30

Agree the management review, corrective action and reporting rhythm.

NIS2
Vodič za rukovodstvo

Pet pitanja, mapa odgovornosti i kontrolna lista za proveru dobavljača.

Radna verzija v0.1 | Septembar 2026.

Ema Petrović | NIS2 Officer | upravljanje sajber bezbednošću i sajber pravo

UPRAVLJAČKI POGLED

Pet pitanja pre liste kontrola

NIS2 postaje koristan kada rukovodstvo može da poveže odluke, odgovornost, dobavljače i dokaze.

01

Šta je zaista u obuhvatu?

Kritične usluge, procesi, podaci, sistemi i zavisnosti.

02

Ko odlučuje i ko nadzire?

Prava odlučivanja, izveštavanje, eskalacija i odobravanje mera.

03

Koji dokaz pokazuje da sistem radi?

Ne samo politike, već odluke, testovi, obuke i korektivne mere.

04

Kako upravljamo rizikom dobavljača?

Kriterijumi, ugovori, dokazi, praćenje i promene rizika.

05

Kako incident stiže do rukovodstva?

Pragovi, uloge i odluke pod vremenskim pritiskom.

MAPA ODGOVORNOSTI

Jedan sistem, više vlasnika

Nijedna funkcija ne može samostalno da sprovede NIS2. Rukovodstvo povezuje odluke i nadzor.

FUNKCIJA	KLJUČNA ODLUKA	PRIMER DOKAZA
Rukovodstvo	Odobrava mere, resurse i prihvatanje rizika.	Odluke, zapisnici, pokazatelji i praćenje korektivnih mera.
Pravni tim	Prevodi obaveze u upravljanje i ugovorne zahteve.	Registar obaveza, ugovorne klauzule, pravna mišljenja.
Nabavka	Ugrađuje sajber kriterijume u izbor i praćenje dobavljača.	Due diligence, kriterijumi, provere, evidencija odstupanja.
Sajber / IT	Projektuje, sprovodi i testira kontrole.	Rezultati testova, logovi, ranjivosti, planovi remedijacije.
Operacije	Obezbeđuju kontinuitet kritičnih usluga.	BIA, planovi kontinuiteta, vežbe i lessons learned.
HR i vlasnici procesa	Definišu uloge, pristup, obuke i ponašanje.	Matrice pristupa, obuke, potvrde uloga i offboarding.

Matrica odgovornosti je korisna samo kada je povezana sa stvarnim odlukama, pragovima izveštavanja i dokazima.

RIZIK DOBAVLJAČA

Ugovor nije kraj provere

Raspodela obaveza na papiru ne uklanja potrebu kompanije da razume i nadzire zavisnost.

Šta proveriti kod dobavljača

- ☐ Koja pravna lica, usluge, sistemi i lokacije ulaze u obuhvat?
- ☐ Ko je izdao dokaz i da li je izdavalac kompetentan i proverljiv?
- ☐ Do kada dokaz važi i kako se prate značajne promene?
- ☐ Koje obaveze prijave incidenta i saradnje postoje u ugovoru?
- ☐ Koji alternativni aranžman postoji ako dobavljač zakaže?

Ako dobavljač navodi ISO/IEC 27001

- ☐ Zatražite kopiju važećeg sertifikata.
- ☐ Proverite sertifikaciono telo i period važenja.
- ☐ Pročitajte obim: da li pokriva konkretnu uslugu?
- ☐ Proverite obuhvaćene lokacije i pravno lice.
- ☐ Zabeležite šta sertifikat ne dokazuje za vaš slučaj.

PRIMER IZ PRAKSE

Zdravstvenoj kompaniji dobavljač je samo rekao da poseduje ISO/IEC 27001. Bez obima, izdavaoca i važenja, ta izjava nije pokazala da sertifikat pokriva konkretnu uslugu na koju se kompanija oslanja. Traženje dokaza nije nepoverenje. To je upravljanje rizikom.

DOKAZI I POČETAK

Od dokumenta do vidljivog sistema

Počnite malim brojem dokaza koji pokazuju odluku, sprovođenje, proveru i poboljšanje.

DOKAZ	VLASNIK	ŠTA TREBA DA POKAŽE
Odluka rukovodstva	Rukovodstvo	Šta je odobreno, na osnovu kojih informacija i uz koje uslove.
Registar rizika	Vlasnik rizika	Rizik, tretman, rok, status i prihvatanje preostalog rizika.
Provera dobavljača	Nabavka / bezbednost	Kritičnost, traženi dokazi, nalazi, odstupanja i praćenje.
Test ili vežba	IT / operacije	Scenario, rezultat, slabosti, vlasnik korektivne mere i rok.
Obuka i uloge	HR / rukovodstvo	Ko mora šta da zna, potvrda učešća i procena razumevanja.

PRVIH 30 DANA

01 **Dani 1-7**

Potvrdite obuhvat, kritične usluge i vlasnike odluka.

02 **Dani 8-14**

Mapirajte postojeće mere i dokaze, ne samo politike.

03 **Dani 15-21**

Razvrstajte dobavljače po kritičnosti i proverite najveće zavisnosti.

04 **Dani 22-30**

Dogovorite upravljački pregled, korektivne mere i ritam izveštavanja.

SOURCES AND USE / IZVORI I NAMENA

A working instrument / Radni instrument

Not a substitute for legal analysis. / Nije zamena za pravnu analizu.

This preview turns the management logic of NIS2 into questions and evidence prompts. Scope and obligations must always be assessed for the specific entity and jurisdiction.

Ova radna verzija prevodi upravljačku logiku NIS2 u pitanja i zahteve za dokazima. Obuhvat i obaveze uvek treba proceniti za konkretan subjekt i pravni okvir.

PRIMARY SOURCES / PRIMARNI IZVORI

01 Directive (EU) 2022/2555, especially Article 20 on management bodies and Article 21 on cybersecurity risk-management measures. / Direktiva (EU) 2022/2555, naročito član 20 o upravljačkim telima i član 21 o merama za upravljanje sajber rizicima: eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

02 ENISA, NIS Directive 2 overview. / ENISA, pregled Direktive NIS 2: enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2

03 ENISA, Good Practices for Supply Chain Cybersecurity. / ENISA, dobre prakse za sajber bezbednost lanca snabdevanja: enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

ABOUT THE AUTHOR / O AUTORKI

Ema Petrović works across responsible AI, digital transformation, NIS2, cyber law and organisational change. Her focus is the space between a formal framework and the decisions, evidence and behaviours that make it work in practice.

Ema Petrović se bavi odgovornom primenom AI, digitalnom transformacijom, NIS2, sajber pravom i organizacionim promenama. U fokusu njenog rada je prostor između formalnog okvira i odluka, dokaza i ponašanja koji ga pretvaraju u praksu.

NIS2 Officer | Cybersecurity governance and cyber law

ema.e.petrovic@gmail.com | blueoceannavigator.com