

distinct
plus prin responsabilitate



Strategia întâlnește realitatea

ISO și NIS2, controlul comun, obligațiile distincte

*„Toată lumea are o strategie până la primul
pumn în gură.”*

– ATRIBUIT LUI MIKE TYSON

Nu un nou strat de birocrație: un punct comun în
care cerințele diferite întâlnesc aceeași organizație.



ISO și NIS2: apropiere fără echivalență

ISO

Disciplină de management

Standard voluntar centrat pe guvernanță internă, bune practici, cicluri PDCA și îmbunătățire continuă a proceselor organizaționale.

NIS2

Obligații legale de reziliență

Regim de conformitate obligatoriu, cu cerințe stricte de securitate cibernetică, răspundere a conducerii și termene rigide de raportare.

ÎMPREUNĂ

Mecanisme reutilizabile

Un control operațional comun susține ambele direcții: aceeași procedură tehnică generează dovezi, dar verificările rămân distincte.

Trei coloane simple, fără semn de egalitate între ele:
un certificat ISO nu este dispensă de la obligațiile legale NIS2.



Controlul: puntea dintre cerințe și realitate

Cum transformăm prevederile formale în acțiuni verificabile la nivelul infrastructurii.

01

Cerință

Prevederea formală din directivă, lege sau standardul aplicabil.

02

Risc

Amenințarea concretă identificată și impactul operațional asupra activității.

03

Control

Măsura tehnică, organizatorică sau procedurală implementată efectiv.

04

Dovadă

Jurnalul, înregistrarea, configurația sau raportul care probează funcționarea.

05

Evaluare

Verificarea periodică a eficacității în raport cu fiecare criteriu specific.

Principiul cheie: Același control poate susține mai multe cerințe, dar nu le face echivalente. Controlul este puntea tehnică; interpretarea rezultatelor rămâne specifică fiecărui cadru de conformitate.



Exemplu: evaluarea unui furnizor critic

Control comun: evaluăm și monitorizăm furnizorul în raport cu riscurile și cerințele aplicabile.

Cadru de referință	Întrebarea centrală a evaluării	Finalitatea analizei
ISO 9001	Poate furnizorul livra consecvent conform cerințelor noastre?	Calitatea și stabilitatea livrabilelor
ISO/IEC 27001	Sunt tratate riscurile de securitate a informației din relația cu el?	Confidențialitatea și integritatea datelor
NIS2	Sunt îndeplinite cerințele aplicabile de securitate a lanțului de aprovizionare?	Reziliența operațională și conformarea legală
CONCLUZIE: UN PROCES ȘI O FIȘĂ COMUNĂ, CRITERII ȘI CONCLUZII DISTINCTE.		



Ce adaugă NIS2 și nu dispare prin integrare

Integrăm munca de zi cu zi, nu declarăm cerințele echivalente.

Domeniu

Obligatoriu prin lege pentru entități esențiale și importante, fără posibilitatea de a exclude servicii critice din perimetru.

Conducere

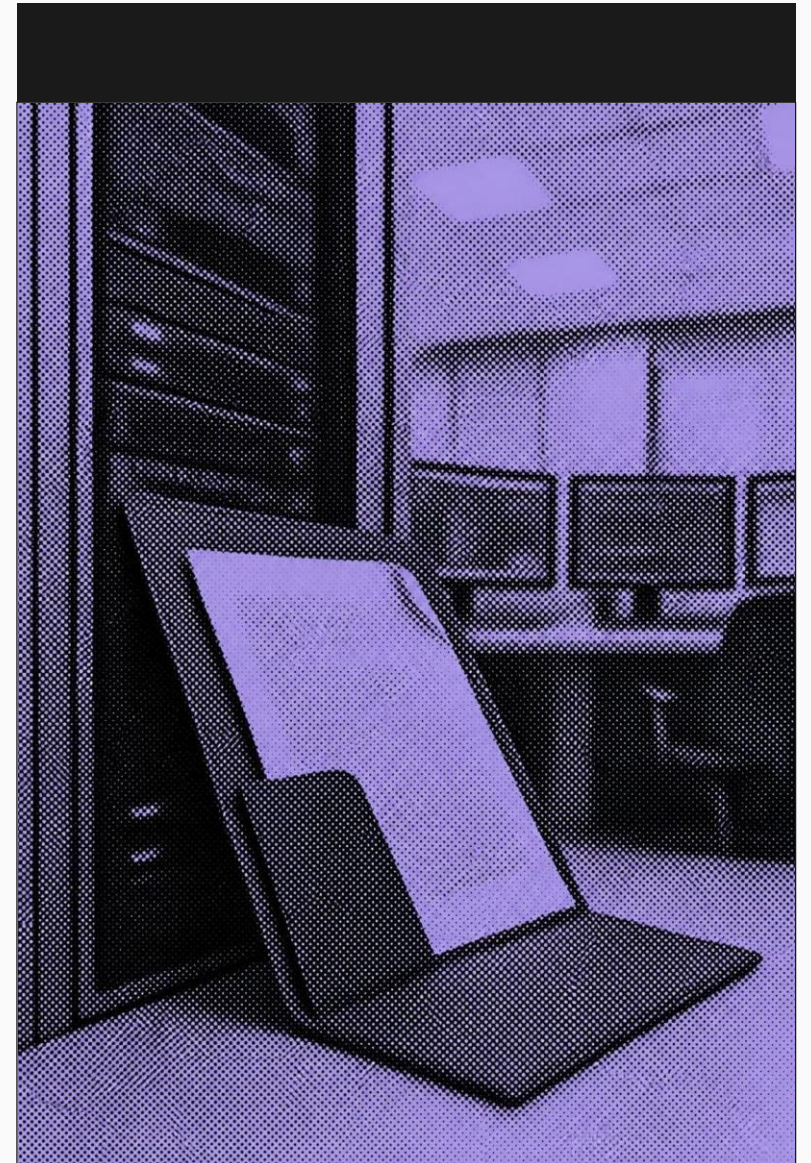
Răspundere directă, personală a organelor de conducere pentru aprobarea și supravegherea măsurilor de securitate.

Raportare

Obligații legale stricte de notificare a incidentelor semnificative (avertizare timpurie în 24h, notificare completă în 72h).

Autoritate

Supraveghere ex-post sau ex-ante din partea autorității competente naționale, cu putere de control și sancțiuni severe.



PRAGUL DINTRE GESTIUNEA INTERNĂ
ȘI MANDATUL PUBLIC



De mâine: o legătură verificabilă, nu încă un dosar

Mecanismul operațional: Cerințe distincte → Control comun → Dovezi relevante → Concluzii distincte

1. Identificați

Cartografiați obligațiile NIS2 direct aplicabile sectorului și entității dumneavoastră.

2. Legați

Uniți fiecare cerință de risc, controlul operațional, responsabilul nominal și dovada existentă.

3. Completați și testați

Acoperiți golurile reale și testați reziliența prin simulări și verificări practice.

„Lucrurile nu sunt greu de făcut, greu este să te pui în starea de a le face.”

— atribuit lui Constantin Brâncuși