TÜV AUSTRIA

HACKOUT Portalul Atacurilor Cibernetice

Securitatea cibernetică – obligație legală. Rolul NIS2 în mediul de afaceri

Rares Macarov

Auditor NIS autorizat DNSC
TUV Austria Cyber Security Manager
TUV Austria Chief Information Security Officer
TUV Austria Data Privacy Officer
IRCA Information Security Trainer
IRCA Information Security Lead Auditor
RINA SIMTEX Information Security Trainer
IQCert Lead Auditor
SUN CERT Information Security Trainer
Member of Cyber Security International Forum
EC-COUNCIL Certified Ethical Hacker
ISECOM Certified Hacker Analyst

De ce securitate cibernetică?

Când atacurile nu mai vizează doar datele, ci continuitatea întregului business.

Peste 80% dintre companiile europene au raportat cel puțin un incident cibernetic în ultimul an
(ENISA Threat Landscape 2024)

Impactul mediu al unui atac major depășește 1,8 milioane € per incident
(IBM Cost of a Data Breach 2024)

9 din 10 atacuri vizează lanțul de aprovizionare sau parteneri externi.

Organizatie	Atac (2025)	Impact
Marks & Spencer (UK)	Ransomware (Scattered Spider)	Site blocat 3 zile, pierderi reputaționale și financiare
Jaguar Land Rover (UK)	Compromitere retea industriala	Productie oprita mai mult de 1 saptamana
Bouygues Telecom (Franta)	Bresa de date	6,4 milioane clienți afectați
Aeroporturi europene	Atac asupra platformei MUSE	Check-in și bagaje blocate în peste 10 aeroporturi

De ce securitate cibernetică?

Când atacurile nu mai vizează doar datele, ci continuitatea întregului business.

Context global

- Expunerea crescută a companiilor la ameninţări sofisticate şi frecvente.
- Impactul real asupra operaţiunilor, reputaţiei dar şi asupra lanţurilor de furnizori.
- Securitatea cibernetică trece de la rolul de „problemă IT” la „obligaţie de business strategică”.

Cadrul legislativ european și național

Strategia UE pentru Era Digitală

NIS 2 - Directiva (UE) 2022/2555

▸ Stabilește cerințe stricte de securitate cibernetică și raportare a incidentelor pentru organizațiile esențiale și importante din statele membre..

Cyber Resilience Act - Regulamentul (UE) 2019/881

▸ Stabilește cerințe obligatorii de securitate cibernetică pentru toate produsele și software-urile cu elemente digitale puse pe piața UE, pentru a asigura protecția utilizatorilor și a rețelelor împotriva vulnerabilităților și atacurilor.

DORA (Digital Operational Resilience Act) - Regulamentul (UE) 2022/2554

▸ Impune cerințe de reziliență operațională digitală instituțiilor financiare, asigurându-le capacitatea de a rezista, răspunde și a se recupera după incidente.

CER (Critical Entities Resilience) – Directiva (UE) 2022/2557

▸ Stabilește măsuri pentru creșterea rezilienței entităților critice din sectoare esențiale, astfel încât acestea să poată preveni, răspunde și recupera după incidente care afectează serviciile vitale

Data Act - Regulamentul (UE) 2023/2854

▸ Stabilește drepturi și obligații privind accesul, partajarea și utilizarea echitabilă a datelor generate de dispozitive și servicii inteligente.

AI Act - Regulamentul (UE) 2024/1689

▸ Stabileşte reguli armonizate pentru sistemele de inteligenţă artificială, în funcţie de nivelul de risc, cu scopul de a sprijini dezvoltarea unei inteligenţe artificiale de încredere.

Cadrul legislativ european și național

Strategia UE pentru Era Digitală

REZILIENȚĂ, SUVERANITATE TEHNOLOGICĂ ȘI LEADERSHIP

- Implementarea Directivei NIS 2.0 la nivelul fiecărui stat membru
- Crearea scutului de securitate cibernetică (CSIRT, SOC)
- Crearea infrastructurii de comunicații sigure
- Crearea de Centre Naționale de Competență și Coordonare în Cyber (CCCN)
- Creșterea competențelor în securitate cibernetică

CREȘTEREA CAPACITĂȚII OPERAȚIONALE DE PREVENIRE, DESCURAJARE ȘI RĂSPUNS

- Crearea cadrului de gestionare a crizelor de securitate cibernetică
- Dezvoltarea principiilor de răspuns la infracționalitatea cibernetică
- Dezvoltarea sistemului de informare reciprocă la nivelul statelor membre în domeniul securității cibernetice
- Dezvoltarea unui cadru de politică de apărare cibernetică

COOPERAREA PENTRU OBȚINEREA UNUI CYBER-SPAȚIU DESCHIS GLOBAL PROTEJAT

- Dezvoltarea politicilor pentru standardizare în domeniul securității cibernetice
- Promovarea unui model de guvernanță a Internetului cu implicarea mai multor părți interesate
- Dezvoltarea agendei de consolidare a capacităților cibernetice
- Dezvoltarea rețelei UE de dialog și diplomație cibernetică

Cadrul legislativ european și național

Strategia națională pentru securitate cibernetică

Strategia Națională de Securitate Cibernetică 2022–2027 - HG nr. 1321/2021

- Definește cadrul strategic pentru protejarea spațiului cibernetic al României
- Vizează creșterea rezilienței digitale și protecția infrastructurilor critice de informații
- Promovează cooperarea între autorități, mediul privat și societatea civilă în prevenirea și gestionarea incidentelor cibernetice
- Este aliniată obiectivelor Uniunii Europene în domeniul securității cibernetice
- Implementarea este coordonată de Directoratul Național de Securitate Cibernetică (DNSC), împreună cu instituțiile și operatorii din sectoarele esențiale.

Cadrul legislativ european și național

De la strategie europeană la obligație națională de conformare.

OUG 155/2024

▸ Transpune Directiva NIS2 în legislația României, stabilind măsuri de securitate cibernetică și obligații de raportare pentru entitățile esențiale și importante din spațiul cibernetic național civil.

Legea nr. 58/2023

▸ Reglementează organizarea, atribuțiile și cooperarea instituțiilor statului în domeniul securității și apărării cibernetice a României, stabilind cadrul legal pentru protejarea spațiului cibernetic național.

HG nr. 271/2023

▸ Stabilește normele de aplicare a Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, definind responsabilitățile instituțiilor și procedurile de cooperare în domeniul apărării cibernetice..

HG nr. 718/2011

▸ Stabilește cerințele și mecanismele de identificare, desemnare și protecție a infrastructurilor critice naționale, asigurând coordonarea măsurilor de securitate pentru funcționarea serviciilor esențiale ale statului.

Legea nr. 362/2018

▸ Stabilește măsuri pentru un nivel comun ridicat de securitate a rețelelor și sistemelor informatice, impunând obligații de securitate și raportare pentru operatorii de servicii esențiale și furnizorii de servicii digitale.

Ordinul DNSC nr. 1323/2020

▸ Stabilește cerințele minime de securitate cibernetică pentru operatorii de servicii esențiale și furnizorii de servicii digitale, precum și măsurile tehnice și organizatorice necesare pentru protejarea rețelelor și sistemelor informatice.

Cadrul legislativ european și național

De la strategie europeană la obligație națională de conformare.

NIS 2 - (Directiva (UE) 2022/2555

- Adoptată de Parlamentul European în decembrie 2022, intrată în vigoare în ianuarie 2023.
- Înlocuiește Directiva NIS (2016), extinzând domeniul de aplicare și responsabilitatea managerială.
- **Ținta:** toate organizațiile esențiale și importante din peste 18 sectoare (energie, transporturi, apă, sănătate, administrație publică, servicii digitale etc.).

Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

NIS 2

- Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2) a fost adoptată în decembrie 2022.

- Transpune lecțiile învățate din NIS (Directiva 2016/1148), extinzând domeniul de aplicare și înăsprind cerințele de conformitate.

Ce aduce nou față de NIS?

NIS (2016)	NIS2 (2022)
Acoperea doar câteva sectoare	Se extinde la **18 sectoare esențiale și importante**
Autoevaluare laxă	**Audituri periodice obligatorii**
Răspundere generală	**Răspundere clară pentru conducere**
Termene vagi de raportare	**24h pentru notificare inițială**, 72h pentru detalii

Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

Obiectiv A Managementul riscurilor de securitate cibernetică	**Obiectiv B** Protecția împotriva atacurilor cibernetice	**Obiectiv C** Detectarea evenimentelor de securitate cibernetică	**Obiectiv D** Minimizarea impactului incidentelor de securitate cibernetică
Obiectiv A Structuri organizaționale, politici și procese adecvate pentru a înțelege, evalua și gestiona sistematic riscurile de securitate cibernetică	**Obiectiv B** Măsuri de securitate proporționale pentru a proteja serviciile și sistemele esențiale împotriva atacurilor cibernetice. Include: controlul identității și accesului, securitatea datelor și a serviciilor, politici și procese de protecție a informațiilor, tehnologie de protecție, conștientizare și instruire.	**Obiectiv C** Capacitățile de a asigura că măsurile de securitate rămân eficiente și de a detecta evenimentele de securitate cibernetică care afectează sau pot afecta serviciile esențiale. Include monitorizarea securității și detectarea anomaliilor.	**Obiectiv D** Capacități de minimizare a impactului incidentului de securitate cibernetică asupra furnizării de servicii esențiale, inclusiv restabilirea acestor servicii. Include planuri de răspuns și recuperare.

Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

Obiectiv A
Managementul riscurilor de securitate cibernetică

- Guvernanță
- Managementul riscurilor
- Managementul resurselor
- Supply chain

Obiectiv B
Protecția împotriva atacurilor cibernetice

- Politici și procese de protecție
- Controlul identității și accesului
- Securitatea datelor
- Securitatea sistemelor
- Sisteme și rețele reziliente
- Instruire și conștientizare

Obiectiv C
Detectarea evenimentelor de securitate cibernetică

- Monitorizarea sistemelor
- Descoperire proactivă a evenimentelor

Obiectiv D
Minimizarea impactului incidentelor de securitate cibernetică

- BCP/DRP
- Învățarea din incidente

Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

Entitate esențială

Persoană fizică sau juridică de drept public sau privat de tipul celor prevăzute în anexa și care furnizează un serviciu esențial.

Un serviciu este considerat esențial dacă furnizarea lui îndeplinește cumulativ următoarele condiții:

a) serviciul este esențial în susținerea unor activități societale și/sau economice de cea mai mare importanță;

b) furnizarea sa depinde de o rețea sau de un sistem informatic;

c) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident.

Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

Cine?

Entități esențiale

- Toate sectoarele acoperite de NIS
- În plus:
  - Servicii farmaceutice
  - Producători, distribuitori de dispozitive medicale
  - Servicii de cloud-computing, data centers
  - Servicii de tratare ape uzate
  - Servicii în domeniul aero-spațial
  - Administrație publică centrală

Entități importante

- Întreprinderi mijlocii
- Servicii ce pot afecta societate, economie, industrie, mediu
- În plus:
  - Servicii de vânzări/distribuție online
  - Producători, distribuitori în domeniul alimentar
  - Servicii poștale și de curierat
  - Servicii de management al deșeurilor
  - Producători în domeniul chimic
  - Industrie importantă – vehicule, transport, echipamente
  - Servicii de furnizare apă potabilă

Cadrul legislativ european și național

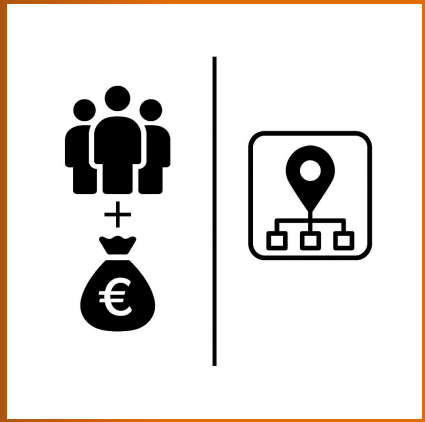
Directiva UE 2022/2555 – NIS2

Entități

- 18 domenii (sectoare) de activitate
- **Esențiale :** Organizații mari cu peste 250 angajați, cifra de afaceri cel puțin 50 mil. EURO
- **Importante :** Organizații cu 50 – 249 angajați, cifra de afaceri mai mare de 10 mil. EURO
- Criteriile sunt cumulative dar pot fi înlocuite de criterii de criticitate a serviciilor/activităților

Angajați ≥ 250
CA ≥ 50.000.000 €

50≤ Angajați < 250
CA < 50.000.000 €



Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

Obligații

Obiectiv	Cerințe NIS 2.0
Securitate	Entitățile esențiale și importante trebuie să implementeze măsuri tehnice și organizatorice pentru a gestiona riscurile la adresa rețelelor și sistemelor informatice
Evaluarea riscurilor	Măsurile tehnice și organizatorice trebuie să fie adecvate și proporționale cu riscurile și să fie "state of the art". Trebuie realizate evaluări de risc periodice pentru menținerea adecvării măsurilor
Măsuri minime obligatorii	Măsurile tehnice și organizatorice minime trebuie să includă: - Prevenirea, detecția și răspunsul la incidente - Continuitatea activităților și managementul crizelor - Achiziția și întreținerea rețelelor și sistemelor în mod sigur, inclusiv gestionarea și raportarea vulnerabilităților - Testarea și auditul de securitate cibernetică - Utilizarea de metode sigure de criptare
Lanțul de aprovizionare	Măsurile tehnice și organizatorice trebuie să fie adecvate și proporționale cu riscurile asociate lanțului de furnizori. Trebuie luate în considerare vulnerabilitățile sistemului de aprovizionare utilizat. Trebuie evaluate riscurile în domeniul furnizării de servicii de stocare a datelor, servicii de transmitere, procesare a informațiilor, servicii de mentenanță IT etc.
Nivel comun	Entitățile trebuie să realizeze periodic audituri de securitate cibernetică, teste de penetrare cu auditori de securitate autorizați. Rapoartele de audit vor fi transmise autorității naționale (DNSC)
Forța de muncă (personalul)	Măsurile tehnice și organizatorice trebuie să includă instruire și conștientizare periodice adecvate ale personalului (propriu și colaborator)
Raportarea incidentelor	Măsurile tehnice și organizatorice trebuie să includă procese/proceduri de notificare a autorităților relevante (DNSC), a clienților și altor părți interesate despre producerea incidentelor de securitate ce pot avea impact semnificativ

Cadrul legislativ european și național

Directiva UE 2022/2555 – NIS2

Obligații

Be secure

Implementarea de măsuri de securitate proportionale si adecvate cu riscurile (abordare bazată pe risc)

Be vigilant

Monitorizarea continuă a sistemelor, rețelelor, echipamentelor, personalului pentru detectarea amenințărilor și prevenirea incidentelor

Be resilient

Implementarea de măsuri adecvate de răspuns la incidente, de revenire și recuperare după un incident

Cadrul legislativ european și național

OUG nr. 155/2024

Obligații

- Implementarea măsuri tehnice și organizatorice de securitate proportionale si adecvate cu riscurile (abordare bazată pe risc)
- Entitățile trebuie să se înregistreze la DNSC în termen de 30 de zile de la intrarea în vigoare a ordonantei
- Raportarea incidentelor de securitate cibernetică către DNSC în termen de 24 de ore (raportare inițială)
- Entitățile transmit evaluarea nivelului de risc a entității către DNSC în termen de 60 de zile de la data comunicării deciziei directorului DNSC
- În termen de 60 de zile de la transmiterea evaluării nivelului de risc, entitățile realizează o autoevaluare a nivelului de maturitate a măsurilor de gestionare a riscurilor de securitate cibernetică și apoi anual
- Entitățile esențiale întocmesc și transmit către DNSC un plan de măsuri pentru remedierea deficiențelor identificate, asumat de managementul entității, în conformitate cu măsurile de gestionare a riscurilor aplicabile acestora
- Entitățile esențiale și entitățile importante sunt obligate să se supună efectuării unui audit de securitate cibernetică în condițiile și cu periodicitatea stabilite prin ordinul directorului DNSC

Cadrul legislativ european și național

OUG nr. 155/2024

Responsabil NIS

- Obligația desemnării unui Responsabil NIS în entitățile esențiale și importante

- Persoana desemnată să coordoneze implementarea cerințelor NIS
- Punct unic de contact între organizație și DNSC / CSIRT Național
- Rol strategic, nu doar tehnic
- Nu trebuie confundat cu alte roluri (ex. DPO)

- Acces direct la conducerea organizației
- Putere de decizie asupra politicilor și procedurilor de securitate
- Dreptul de a solicita informații de la toate departamentele
- Autoritatea de a verifica implementarea măsurilor NIS
- Posibilitatea de a aloca sau propune resurse (buget, personal, tehnologie)

Cadrul legislativ european și național

OUG nr. 155/2024

Raportarea incidentelor

de la data la care au luat cunoștință de incidentul semnificativ, o avertizare timpurie care, după caz, indică dacă există suspiciuni că incidentul semnificativ este cauzat de acțiuni ilegale sau răuvoitoare sau ar putea avea un impact transfrontalier

din momentul în care au luat cunoștință de incidentul semnificativ, o notificare a incidentului, se prezintă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili;

La cerere — **Raport intermediar** privind actualizarea relevantă a situației (solicitare venită din partea CSIRT sau autoritate competentă)

30 zile — **Raport final**
sau dacă incidentul se desfășoară la momentul raportului final, un raport de progres și un raport final la 1 lună de la încheiere

Auditul de securitate cibernetică

DNSC poate:

a) **derula activități de supraveghere, verificare și control** efectuate de persoane desemnate în acest sens prin decizie a directorului DNSC;

b) **dispune efectuarea de audituri de securitate ad-hoc**, realizate de un auditor de securitate cibernetică atestat;

c) solicita informații necesare pentru a evalua măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate

d) solicita acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor de supraveghere;

e) solicita date, documente și orice informații care atestă punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate cibernetică efectuate de un auditor atestat și mijloacele de probă care stau la baza acestora.

Auditul de securitate cibernetică

În cel mult **15 zile lucrătoare** de la data primirii raportului de audit, entitățile sunt obligate să întocmească și să transmită către DNSC, în baza recomandărilor emise de către auditor, planul de măsuri pentru remedierea tuturor deficiențelor constatate și termenele asumate pentru implementarea acestora

Entitățile sunt obligate să implementeze planul de măsuri în termenul asumat

Entitatea în cauză notifică DNSC cu privire la implementarea tuturor măsurilor prevăzute și pune la dispoziție acte doveditoare în acest sens, în cel mult **5 zile** de la împlinirea termenului asumat

Cadrul legislativ european și național

OUG nr. 155/2024

Sancțiuni

DNSC aplică următoarele sancțiuni:

a) avertisment;

b) amendă contravențională.

10 000 000 EUR sau o limită superioară de cel puțin 2 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține **ENTITATEA ESENȚIALĂ**, luându-se în considerare valoarea cea mai mare dintre acestea.

7 000 000 EUR sau având o limită superioară de cel puțin 1,4 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține **ENTITATEA IMPORTANTĂ**, luându-se în considerare valoarea cea mai mare dintre acestea.

TÜV AUSTRIA

NIS2 în mediul de afaceri

De la problemă IT la responsabilitate strategică

HACKOUT Portalul Atacurilor Cibernetice

Cum schimbă NIS2 cultura organizațională

- NIS2 mută securitatea cibernetică **din zona tehnică în zona de guvernanță**.
- Conducerea devine **direct responsabilă juridic** pentru deciziile și măsurile de securitate.
- Securitatea cibernetică este acum un **subiect de board**, nu doar de departament IT.
- Cultura organizațională se schimbă: accent pe **conștientizare, responsabilitate și transparență**.

NIS2 în mediul de afaceri

Impactul asupra mediului de afaceri

Cum transformă NIS2 relațiile comerciale și competitivitatea

Domeniu	Schimbare generată de NIS2	Beneficiu concret
Managementul riscului	Introduce analiza și tratamentul riscurilor cibernetice la nivel strategic	Decizii mai informate și prioritizare eficientă
Guvernanță corporativă	Implicarea consiliului de administrație în securitate	Responsabilitate clară și raportare periodică
Parteneriate și contracte	Se cer garanții de securitate (due diligence NIS2)	Acces la contracte și licitații
Imagine și reputație	Demonstrează conformitate legală și transparență	Crește încrederea partenerilor, investitorilor și autorităților

NIS2 în mediul de afaceri

Compania care a devenit mai puternică după NIS2

„SecureTrans Logistics” – de la audit la avantaj competitiv

Situația inițială: lipsa politicilor de securitate, incidente frecvente, pierdere de încredere.

Acțiuni implementate:

- analiză de risc și plan de răspuns la incidente;
- politici și instruiri interne;
- audit și monitorizare continuă.

Rezultate după 12 luni:

- zero incidente critice;
- certificare ISO 27001;
- câștigarea unui contract internațional datorită conformității NIS2

Etapele de conformare

1. Identificarea domeniului de aplicare
•Determinarea dacă organizația este *entitate esențială* sau *importantă*.
•Stabilirea activelor și serviciilor critice.

2. Evaluarea riscurilor și activelor critice
•Analiza vulnerabilităților, interdependențelor și impactului.
•Utilizarea metodologiilor ISO/IEC 27001, 27005, 31000, 22301.

3. Elaborarea politicilor și procedurilor interne
•Politici de securitate, control al accesului, clasificare a informațiilor.

4. Implementarea măsurilor tehnice și organizatorice
•Conform art. 21 din NIS2: control acces, criptare, segmentare rețea, backup.

5. Crearea planului de răspuns la incidente
•Definirea fluxului de raportare către DNSC și a echipei interne de răspuns.

6. Raportare și audit periodic
•Revizuire anuală a controalelor și raportare a incidentelor.

Rolul furnizorilor SOC / CSIRT / MSSP

Parteneri strategici în asigurarea conformității

Tip furnizor	Rol în conformitate	Beneficii principale
SOC (Security Operations Center)	Monitorizează permanent evenimentele și alertele de securitate	Detectare timpurie și răspuns rapid la incidente
CSIRT (Computer Security Incident Response Team)	Coordonare tehnică și procedurală în timpul incidentelor	Limitarea impactului și prevenirea recurenței
MSSP (Managed Security Service Provider)	Oferă servicii integrate (monitorizare, firewall, EDR/XDR, SIEM, IDS/IPS etc.)	Cost redus față de resurse interne, scalabilitate

Cum se raportează NIS2 la alte norme

Corelare între NIS2 și principalele standarde și reglementări

Domeniu / Obiectiv	NIS2	ISO 27001	ISO 27005	ISO 22301	DORA	GDPR
Guvernanță și responsabilitate	✔ conducerea răspunde legal	✔ clauze 4–7	–	✔ responsabilități BCM	✔ responsabilitate management	✔ art. 24–25
Managementul riscurilor	✔ obligatoriu	✔ Clauza 6, 8, Anexa A	✔ proces complet de analiză	✔ analiza riscurilor de întrerupere	✔ analiza riscurilor IT&C	✔ evaluare riscuri date personale
Planificare și continuitate	✔ planuri de răspuns la incidente	✔ Clauza 6, Anexa A	✔ planificarea si tratarea riscurilor	✔ planuri de continuitate	✔ testare reziliență	✔ notificare încălcare
Raportare și audit	✔ raportare DNSC, audit periodic	✔ Audit intern	✔ monitorizare riscuri	✔ revizuire periodică BCM, audit intern	✔ raportare incident	✔ notificare ANSPDCP
Conformitate și sancțiuni	✔ OUG 155/2024 – amenzi	✔ Opțional (certificare)	–	✔ Opțional (certificare)	✔ reglementare financiară	✔ amenzi RGPD

Beneficiile cadrului integrat și aplicarea practică

De la conformare la valoare adăugată prin integrarea normelor

- Adoptarea unui cadru integrat (NIS2 + ISO + DORA + GDPR) oferă:

✅ **coerență** – reguli și controale unificate între departamente;
✅ **eficiență** – eliminarea dublurilor de audit și documentație;
✅ **credibilitate** – demonstrarea conformității față de clienți și autorități;
✅ **reziliență** – integrarea managementului continuității (ISO 22301).

- **Exemple practice:**

- Politicile ISO 27001 pot fi folosite pentru a demonstra conformitatea cu NIS2.
- Procesul de evaluare a riscurilor din ISO 27005 acoperă cerințele DNSC pentru raportare.
- Testele de continuitate și exercițiile BCM (ISO 22301) sprijină cerințele de reziliență NIS2.

Provocările actuale în aplicarea NIS2

Provocări reale în drumul spre conformitate

Resurse umane
- Lipsa specialiștilor în securitate cibernetică și conformitate.
- **Impact:** Întârzieri în implementare, dependență de consultanți externi.

Buget și percepție
- Investițiile în securitate sunt văzute ca „pierdere”, nu protecție.

Impact: Subfinanțare, prioritizare greșită a riscurilor.

Cultură organizațională
- Lipsă de conștientizare la toate nivelurile.
- **Impact:** Vulnerabilități umane persistente, erori operaționale.

Complexitatea cerințelor
- Lipsa unei viziuni integrate între NIS2, GDPR, ISO etc.
- **Impact:** Suprapuneri, confuzii, lipsă de coordonare.

TÜV AUSTRIA

HACKOUT Portalul Atacurilor Cibernetice

Viitorul este digital. Securitatea trebuie să fie umană.