https://www.zf.ro/info/nis2-si-rolul-cadrului-grc-in-consolidarea-securitatii-cibernetice-a-22943284

ZIARUL FINANCIAR

NIS2 şi rolul cadrului GRC în consolidarea securităţii cibernetice a companiilor

Opinia Specialistului



Autor: Gheorghe Maracine, Manager Departament de Audit şi evaluare Riscuri, Safetech Innovations

05.11.2025, 09:00 61

Odată cu intrarea în vigoare a noii directive NIS2, organizaţiile din sectoarele esenţiale şi importante trebuie să adopte o abordare integrată a guvernanţei şi riscurilor cibernetice. În următoarele rânduri voi aborda modul în care cadrul GRC (Governance, Risk Management & Compliance) contribuie la conformitate şi securitate, deoarece atunci când businessul este protejat şi funcţiile esenţiale sunt garantate, conformitatea devine o consecinţă firească. Serviciile de consultanţă GRC ajută companiile să îşi clarifice responsabilităţile, să reducă riscurile cibernetice şi să se alinieze cerinţelor NIS2.

În domeniul securităţii cibernetice, GRC oferă un cadru integrat prin care organizaţiile pot gestiona în mod coerent guvernanţa, riscurile şi conformitatea. Practic, GRC ajută companiile să definească clar responsabilităţile, să evalueze şi să reducă riscurile cibernetice şi să demonstreze conformitatea cu cerinţele legale. Pentru alinierea la cerinţele NIS2, serviciile de consultanţă GRC oferite de Safetech Innovations sprijină implementarea unei structuri clare de guvernanţă a securităţii, facilitează monitorizarea continuă a riscurilor şi asigură alinierea la obligaţiile de raportare şi control impuse de reglementare. Astfel, organizaţiile pot construi o strategie de securitate solidă, bazată pe transparenţă, responsabilitate şi îmbunătăţire continuă.

Impactul Directivei NIS2 asupra organizaţiilor din România şi principalele provocări

Transpunerea Directivelor NIS şi NIS2 la nivel naţional, iniţial prin Legea nr. 362/2018 şi ulterior prin Legea nr. 124/2025 care aprobă Ordonanţa de Urgenţă a Guvernului nr. 155/2024, reprezintă un pas important pentru consolidarea securităţii cibernetice. Are o contribuţie semnificativă la consolidarea cadrului legislativ naţional şi la creşterea gradului de conştientizare în rândul entităţilor vizate privind necesitatea protejării infrastructurii IT&C. Toate organizaţiile trebuie să ştie că NIS2 aduce schimbări majore prin extinderea domeniului de aplicare, introducerea unor cerinţe mai complexe şi stabilirea unui regim clar de sancţiuni pentru neconformitate.

În România, cea mai mare provocare nu este însă doar complexitatea noilor obligaţii, ci şi lipsa resurselor şi a expertizei interne pentru o implementare corectă. Tragem şi pe această cale un semnal de alarmă că alinierea la cerinţele impuse de NIS2 necesită o abordare strategică şi investiţii susţinute în securitatea şi reziliența cibernetică.

Importanţa adoptării unui cadru solid de GRC în implementarea cerinţelor NIS2

Un cadru GRC integrează procesele de guvernanţă, management al riscurilor şi conformitate, oferind o bază solidă pentru funcţionarea unei organizaţii. Guvernanţa oferă claritate privind direcţia strategică adoptată pentru îndeplinirea obiectivelor sale prin răspunsuri la întrebările-cheie precum cine, ce, de ce, cum, unde şi când.

Managementul riscului este esenţial pentru reducerea nivelului de risc, contribuind la un climat organizaţional sigur. În acelaşi timp, procesul de conformitate garantează alinierea la cerinţele legale şi protejează organizaţia de sancţiuni.

În acest context, adoptarea unui cadru GRC robust este esenţială pentru a asigura transparenţă, control şi trasabilitate, aspecte fundamentale şi pentru implementarea cerinţelor NIS2. Pe termen lung, un astfel de cadru sprijină eficienţa operaţională şi contribuie la reducerea costurilor generate de incidente şi neconformităţi.

Principalele diferenţe dintre vechea directivă NIS şi noua NIS2

Extinderea domeniului de aplicare, introducerea unor cerinţe mai complexe şi stabilirea unui regim clar de sancţiuni pentru neconformitate sunt principalele schimbări aduse de NIS2. Directiva pune accent mai mult pe prevenţie, pe securizarea lanţului de aprovizionare, consolidarea rezilienţei cibernetice, raportarea incidentelor şi responsabilizarea conducerii.

Domeniul de aplicare a fost extins cu sectoarele de gestionare a apelor uzate şi a deşeurilor, fabricare de produse farmaceutice, chimice şi de dispozitive medicale, producţie şi distribuţie de alimente, servicii digitale (platforme de reţele sociale şi servicii de centre de date), furnizori de reţele sau servicii publice de comunicaţii electronice, industrie aerospaţială, servicii poştale şi de curierat, administraţie publică.

NIS2 transformă obligaţiile de conformitate din cadrul relativ general al NIS1, într-un set mai strict, uniform şi aplicabil unui număr semnificativ mai mare de organizaţii.

Rolul Safetech Innovations în alinierea organizaţiilor la NIS2

Safetech Innovations acţionează ca un partener strategic pentru organizaţiile care intră sub incidenţa NIS2. Nu ne limităm la consultanţă punctuală, ci oferim sprijin complet, de la evaluarea iniţială a gradului de conformitate şi identificarea direcţiilor de îmbunătăţire pentru obţinerea acesteia, până la implementarea măsurilor necesare şi monitorizarea continuă a eficienţei lor.

Experienţa noastră în proiecte de anvergură atât naţionale, cât şi internaţionale, ne permite să combinăm cunoştinţele tehnice cu înţelegerea cerinţelor legislative. În acest fel, asigurăm organizaţiilor nu doar conformitatea, ci şi capacitatea de a-şi menţine reziliența cibernetică pe termen lung.

Rolul serviciilor de consultanţă GRC ale Safetech Innovations în managementul riscurilor de securitate cibernetică

Serviciile de consultanţă GRC oferite de Safetech sprijină organizaţiile în evaluarea şi reducerea riscurilor de securitate cibernetică prin aplicarea unor metodologii recunoscute la nivel internaţional, precum ISO, NIST sau COBIT.

Pe lângă aceste cadre, realizăm analize personalizate pentru fiecare industrie, ţinând cont de specificul operaţional şi de reglementările aplicabile. Prin aceste analize, identificăm riscurile relevante şi le prioritizăm pe cele critice, urmând elaborarea unor planuri concrete de remediere care să permită reducerea expunerii şi creşterea rezilienţei organizaţiei.

Etapele esenţiale pentru conformarea companiilor cu NIS2

Este important ca orice organizaţie să implementeze un sistem de management al securităţii informaţiei (SMSI), bazat pe politici, procese, roluri, responsabilităţi şi controale interne bine definite şi respectate, având ca scop gestionarea securităţii informaţiilor.

O analiză a diferenţelor (gap analysis) aplicată acestui cadru SMSI reprezintă punctul de plecare în evaluarea nivelului de conformitate cu cerinţele NIS2. Rezultatul acestei analize evidenţiază diferenţa dintre situaţia actuală a organizaţiei şi cerinţele impuse de directivă, concretizată într-un plan de măsuri ce trebuie implementat pentru atingerea conformităţii.

În funcţie de rezultat, planul poate include măsuri tehnice şi organizatorice precum îmbunătăţirea politicilor şi procedurilor, consolidarea procesului de management al riscurilor, programe de formare şi conştientizare, monitorizare şi audit periodic.

Organizaţiile care trebuie să acorde o atenţie sporită conformării cu NIS2

Entităţile vizate de legislaţie sunt împărţite în două categorii: esenţiale şi importante, ele fiind definite în anexele directivei. Este vorba în principal de organizaţii din sectoare critice, entităţi din lanţurile de furnizare ale acestora, precum şi organizaţii care, prin natura activităţii lor, pot provoca perturbări majore în furnizarea serviciilor.

Este important de ştiut însă că cerinţele aplicabile acestor entităţi pot servi ca un ghid valoros pentru toate organizaţiile expuse riscurilor cibernetice, care doresc să îşi îmbunătăţească postura de securitate cibernetică.

Rolul expertizei Safetech Innovations în eficientizarea proceselor GRC

Expertiza Safetech Innovations în domeniul securităţii cibernetice accelerează şi eficientizează implementarea cerinţelor GRC prin combinarea know-how-ului tehnic cu instrumente proprii de automatizare, precum soluţia iSAM – Information Security Automation Manager, despre care sunt disponibile detalii suplimentare pe website-ul nostru, în secţiunea Produse.

Anii de experienţă ne ajută să conturăm soluţii integrate, acoperind toate etapele, de la consultanţă strategică şi audit, până la implementarea soluţiilor tehnice şi furnizarea de servicii de securitate

gestionate (MSSP). Mai mult, experienţa acumulată în gestionarea incidentelor de securitate ne permite să adaptăm rapid controalele şi politicile GRC la riscurile curente, nu doar la cerinţele formale. Astfel, clienţii beneficiază nu doar de conformitate, ci şi de o creştere reală a rezilienţei cibernetice.

Safetech Innovations este un partener complet, capabil să ofere nu doar consultanţă, ci şi implementare operaţională integrată pentru conformitatea cu NIS2. Cu o experienţă solidă în protejarea infrastructurilor critice şi a organizaţiilor esenţiale din România şi având peste 50 de clienţi aflaţi sub incidenţa NIS, Safetech reuneşte expertiză strategică GRC şi competenţe tehnice avansate pentru a livra soluţii end-to-end ce includ evaluarea gradului de conformitate, implementarea sistemelor tehnice necesare şi monitorizarea continuă prin propriul centru SOC.

Safetech oferă o abordare modulară şi personalizată, adaptată profilului fiecărei organizaţii – de la entităţi esenţiale din energie, transport sau sănătate, până la companii private din domenii reglementate. Echipa de consultanţi GRC lucrează direct cu managementul şi consiliul director pentru a integra cerinţele NIS2 în guvernanţa organizaţională, asigurând nu doar conformitatea formală, ci şi sustenabilitatea pe termen lung a proceselor de securitate.

Alegerea Safetech Innovations ca partener pentru consultanţă GRC pentru îndeplinirea cerinţelor NIS2 înseamnă siguranţă, expertiză locală şi eficienţă în implementare. Cu peste un deceniu de experienţă în securitate cibernetică şi un ansamblu de echipe certificate, Safetech oferă organizaţiilor servicii pentru conformarea cu NIS2 şi un cadru durabil de guvernanţă, risc şi conformitate.

NIS2 nu este doar o cerinţă de conformitate, ci o investiţie strategică

Este esenţial ca această directivă să fie privită ca o schimbare de mentalitate, trecând de la reacţie la prevenţie şi de la protecţie la rezilienţă şi încredere digitală.

NIS2 nu reprezintă doar un set de cerinţe, ci un cadru de transformare organizaţională care încurajează companiile să-şi consolideze procesele interne, să-şi cunoască mai bine riscurile şi să devină mai reziliente în faţa ameninţărilor cibernetice.

Dincolo de aceste aspecte, alinierea la cerinţele NIS2 poate propulsa organizaţia pe scara încrederii, prin consolidarea reputaţiei şi a credibilităţii în faţa partenerilor şi clienţilor.

Într-un context în care atacurile cibernetice sunt tot mai frecvente, consider un avantaj real ca organizaţiile să privească această aliniere ca pe o oportunitate strategică, care le poate aduce beneficii concrete de încredere, competitivitate şi rezilienţă cibernetică pe termen lung.

Gheorghe Mărăcine este Manager al Departamentului de Audit şi Evaluare Riscuri din cadrul Safetech Innovations, companie românească de securitate cibernetică, listată la Bursa de Valori Bucureşti, care sprijină organizaţiile să îşi protejeze infrastructura IT, datele critice şi continuitatea operaţională.

ZIARUL FINANCIAR

Contact Publicitate Termeni şi condiţii Politica de confidenţialitate Politica de cookies Versiunea mobilă