Governance, Risk and Compliance (GRC) platforma

Zakon o kibernetičkoj sigurnosti (NN 14/2024) – NIS2 i EU Uredba 2023/2854 – *Cyber Resilience Act* (CRA) zahtijevaju ulaganja, timski pristup i stalno praćenje pokazatelja – neusklađenost direktno utječe na poslovanje, reputaciju i prihode.

	NIS2 / Zakon o kibernetičkoj sigurnosti	***Cyber Resilience Act* (CRA)**
Fokus	Organizacije i sektorski operatori	ICT proizvodi i softver
Obveznici	Ključni i važni subjekti (energetika, financije, zdravstvo…)	Proizvođači, distributeri, uvoznici, korisnici ICT proizvoda
Obveze	Upravljanje rizicima, 13 mjera, samoprocjena/revizija, prijava incidenata	Sigurnosni zahtjevi za proizvode, sigurnosne nadogradnje, prijava incidenata, sigurnosna dokumentacija
Rokovi	Kategorizacija do 2/2025., usklađenost do 2/2026.	Puna primjena do 1/2027. (incidenti od 10/2025.)
Rizici neusklađenosti	Kazne do 10 mil. € ili 2% prometa, reputacijski rizik, operativni prekidi	Zabrana stavljanja proizvoda na tržište, financijski gubici, pravna odgovornost
Utjecaj na poslovanje	Potreba za GRC sustavom, dodatni troškovi i resursi za usklađenost	Rizici pri nabavi i korištenju neusklađenih proizvoda, povećani troškovi podrške i migracija

GRC platforma centralizira evidenciju mjera, omogućuje revizijski zapis (*audit trail*), automatizirano praćenje statusa provedbe i brzo generiranje izvještaja za nadzorna tijela. Omogućuje jedinstveno praćenje usklađenosti u više zemalja, mapiranje nacionalnih i EU zahtjeva, te digitalnu pohranu dokaza.

Značajke

- Jedinstvena baza mjera, kontrola i dokaza.
- Automatizirani tokovi rada (*workflows*) za korektivne i preventivne radnje (*Corrective And Preventive Actions* - CAPA).
- Nadzorne ploče u stvarnom vremenu omogućuju prikaz ključnih podataka i metrika te praćenje Ključnih pokazatelja izvršenja (KPI) i Ključnih pokazatelja rizika (KRI).
- Integracija s *Information Technology Service Management* (ITSM), *Security Information and Event Management* (SIEM), *Data Loss Prevention* (DLP) sustavima.

Ključne koristi

- Spremnost na revizije i nadzore.
- Smanjenje regulatornog rizika.
- Povećanje sigurnosti i optimizacija procesa.

CRA modul u GRC alatu

CRA modul GRC alata omogućuje automatizirano usklađivanje s CRA regulativom – uključuje sigurnosna testiranja, samoprocjene i pripremu za certifikaciju.

Za usklađenost je potrebno više od 10 stručnjaka različitih profila (pravni, tehnički, sigurnosni, organizacijski). GRC alat objedinjavanjem mjera i normi smanjuje trošak i rizik.

Mogućnosti

- Jedinstveni, alatom potpomognuti modul za usklađenost s CRA regulativom.
- Automatizacija, transparentnost i revizija procesa.
- Efikasan pristup CRA zahtjevima, posebno za manje subjekte čija je agilnost strateška prednost.
- Smanjenje operativnog rizika i troškova usklađivanja uz ubrzano vrijeme do tržišta.

13 mjera i GRC

Mjera 1 – Predanost i odgovornost odgovornih osoba

Definicija: Imenovanje i osnaživanje odgovornih osoba, jasno definirane odgovornosti
GRC: Upravljanje politikama i upravljanje korisnicima sa revizijskim tragom (*Policy Management* + *User Management w/ audit trail*)
Koristi: Transparentnost i odgovornost

Mjera 2 – Upravljanje imovinom

Definicija: Evidencija programske i sklopovske imovine
GRC: Upravljanje imovinom (*Asset Management*) s kategorizacijom po kritičnosti
Koristi: Potpuna vidljivost i kontrola

Mjera 3 – Upravljanje rizicima

Definicija: Identifikacija, analiza, tretiranje rizika
GRC: Upravljanje rizicima (*Risk Management*) s ocjenjivanjem i grafičkim prikazom toplinske skale (*heatmap*)
Koristi: Prioritizacija resursa

Mjera 4 – Sigurnost ljudskih potencijala i identiteta

Definicija: Provjere osoblja, obuke, kontrola pristupa
GRC: Evidencija pristupa i treninga
Koristi: Smanjenje unutarnjih prijetnji

Mjera 5 – Osnovne prakse higijene

Definicija: Zakrpe, antivirus, konfiguracije
GRC: Lista usklađenosti i izvještavanje o sigurnosnim zakrpama (*Compliance checklists and patch reporting*)
Koristi: Smanjenje ranjivosti

Mjera 6 – Sigurnost mreže

Definicija: Segmentacija, monitoring
GRC: Integracija sa *Security Information and Event Management* (SIEM) i mrežna nadzorna ploča (*dashboard*)
Koristi: Brza detekcija prijetnji

Mjera 7 – Kontrola pristupa

Definicija: Ograničavanje i evidencija pristupa
GRC: Pristupni zapisnici (*Access logs*) + *Identity and Access Management* (IAM) integracija
Koristi: Prevencija neovlaštenog pristupa

Mjera 8 – Sigurnost lanca opskrbe

Definicija: Procjena i praćenje dobavljača
GRC: Modul za praćenje i ocjenjivanje dobavljača (*Vendor Management module w/ scoring*)
Koristi: Smanjenje rizika trećih strana

Mjera 9 – Sigurnost razvoja

Definicija: Sigurnosni zahtjevi u *Software Development Life Cycle* (SDLC)
GRC: Upravljanje poslovnim promjenama (*Change management*) i test evidencija
Koristi: Smanjenje ranjivosti koda

Mjera 10 – Kriptografija

Definicija: Upravljanje ključevima i algoritmima
GRC: Evidencija kripto-politika
Koristi: Zaštita podataka

Mjera 11 – Upravljanje incidentima (*Incident management*)

Definicija: Detekcija, analiza, izvještavanje
GRC: Radni tokovi incidenata (*Incident workflow*) + *Security Information and Event Management* (SIEM) integracija
Koristi: Brza reakcija

Mjera 12 – Kontinuitet poslovanja

Definicija: Planovi oporavka i kriznog upravljanja
GRC: *Business Continuity Management* (BCM) modul s testnim scenarijima
Koristi: Održavanje poslovanja

Mjera 13 – Fizička sigurnost

Definicija: Zaštita prostora i opreme
GRC: Evidencija inspekcija i planova
Koristi: Prevencija fizičkih prijetnji

Jedan alat, potpuna kontrola – javite nam se!

ent.company@ericssonnikolatesla.com