ORDINUL

Nr. xxx/zz.ll.aaaa
pentru aprobarea criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților

Având în vedere dispozițiile art. 10 alin. (2) și ale art. 18 din Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, dispozițiile art. 5 lit. b) și ale art. 7 alin. (3) - (4) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022, cu modificările ulterioare,

Directorul Directoratului Național de Securitate Cibernetică emite prezentul Ordin:

Art. 1 – (1) Entitățile, astfel cum acestea sunt definite la art. 4 lit. f) din Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, care nu au fost calificate drept entități esențiale sau entități importante conform art. 5 alin. (1) lit. a), c) - f), alin. (2)-(4), art. 6 alin. (1) și alin. (2) lit. b) și c) și nici conform art. 9 lit. a) și d) din același act normativ, realizează evaluarea gradului de perturbare a serviciilor în vederea completării informațiilor solicitate conform ordinului directorului Directoratului Național de Securitate Cibernetică pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor.
(2) Prin perturbare a unui serviciu, în înțelesul prezentului ordin, se înțelege întreruperea, respectiv afectarea confidențialității sau a modului de funcționare a serviciului respectiv.
(3) Atunci când se realizează evaluarea gradului de perturbare, entitățile se raportează la toate serviciile pe care le prestează și care se încadrează în Anexele nr. 1 și 2 la Ordonanța de urgență a Guvernului nr. 155/2024.

Art. 2 – Rezultatele autoanalizei privind faptul că entitatea este singurul furnizor al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice, conform dispozițiilor art. 9 lit. a) din Ordonanța de urgență a Guvernului nr. 155/2024, astfel cum acestea au fost transmise în aplicarea ordinului pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor emis în temeiul dispozițiilor art. 18 din același act normativ, se interpretează în conformitate cu prevederile art. 5 alin. (1) lit. b), respectiv conform prevederilor art. 6 alin. (2) lit. a) din actul normativ menționat anterior, astfel:
a) o entitate care este unic furnizor în România al unui serviciu prevăzut în Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 este entitate esențială dacă nu a fost identificată astfel conform celorlalte criterii prevăzute la art. 5 din același act normativ;
b) o entitate care este unic furnizor în România al unui serviciu prevăzut în Anexa nr. 2 la Ordonanța de urgență a Guvernului nr. 155/2024 este entitate importantă dacă nu a fost identificată astfel conform celorlalte criterii prevăzute la art. 6 din același act normativ.

Art. 3 – Se aprobă Criteriile și pragurile de determinare a gradului de perturbare a unui serviciu, prevăzute în Anexa nr. 1 la prezentul ordin.

Art. 4 – (1) Se aprobă Metodologia privind evaluarea nivelului de risc, prevăzută în Anexa nr. 2 la prezentul ordin.

(2) Utilizarea metodologiei prevăzute la alin. (1) are scopul de a determina categoria de măsuri tehnice, operaționale și organizatorice destinate identificării, evaluării și gestionării riscurilor aferente securității rețelelor și a sistemelor informatice pe care entitatea trebuie să le implementeze.

(3) În vederea determinării nivelului de risc al entității, Directoratul Național de Securitate Cibernetică, în continuare DNSC, stabilește un scor de bază pentru fiecare sector din fiecare anexă la Ordonanța de urgență a Guvernului nr. 155/2024. Scorul final obținut de către entitate determină nivelul de complexitate a măsurilor de securitate, aferent standardului Cyber Fundamentals.

Art. 5 – (1) Entitățile își calculează scorul prevăzut la art. 3 utilizând formulele de calcul prevăzute în Anexa nr. 2, pornind de la valorile de bază aferente sectorului din care fac parte, prevăzute în cadrul anexei la Metodologia privind evaluarea nivelului de risc al entităților, și în conformitate cu dimensiunea acestora.

(2) O entitate care desfășoară activități în mai multe sectoare își evaluează nivelul de risc aferent fiecărui sector și implementează nivelul de măsuri de securitate corespunzător celui mai mare scor obținut.

(3) Atunci când, urmare a evaluării realizate de către entitate, valorile aferente impactului și probabilității la nivelul propriei organizații ale riscurilor prevăzute în metodologie diferă de valorile de bază ale sectorului cu privire la care se raportează evaluarea, entitatea transmite către DNSC o analiză care cuprinde câte o motivare temeinică pentru fiecare valoare cu privire la care aceasta solicită modificarea valorii de bază.

(4) Urmare a solicitării prevăzute la alin. (3), DNSC poate valida propunerile înaintate de către entitate prin solicitarea transmisă. În situația validării acestora, calculul scorului care determină nivelul de risc al entității se realizează conform valorilor astfel actualizate.

Art. 6 – Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Directorul Directoratului Național de Securitate Cibernetică

Dan - Petre CÎMPEAN

Anexa nr. 1

Criterii și praguri de determinare a gradului de perturbare a unui serviciu

Art. 1 – (1) Impactul, astfel cum acesta este prevăzut la art. 9 din Ordonanța de urgență a Guvernului nr. 155/2024, se clasifică în:

a) impact ridicat – atunci când perturbarea serviciului are consecințe foarte grave și catastrofale, la nivel național, asupra rețelelor și sistemelor informatice, activelor, persoanelor, statului, funcționării serviciilor intersectoriale, sau a funcționării serviciilor transfrontaliere în UE;

b) impact mediu - atunci când perturbarea serviciului are consecințe grave, la nivel național, asupra rețelelor și sistemelor informatice, activelor, persoanelor, statului, funcționării serviciilor intersectoriale, sau a funcționării serviciilor transfrontaliere în UE;

c) impact scăzut - atunci când perturbarea serviciului are consecințe scăzute, la nivel național, asupra rețelelor și sistemelor informatice și activelor entității, asupra persoanelor, statului, funcționării serviciilor intersectoriale, sau a funcționării serviciilor transfrontaliere în UE. Consecințele scăzute se referă la afectarea capacității unei entități de a își îndeplini misiunea sau obiectivele sale într-o asemenea măsură încât aceasta să fie capabilă să își îndeplinească funcțiile principale, dar reduce semnificativ eficacitatea acestor funcții.

(2) Nivelul impactului, astfel cum acesta este prevăzut la alin. (1), se determină având în vedere următoarele:

a) drepturile și libertățile fundamentale;

b) economia națională;

c) sănătatea și viața persoanelor;

d) impactul financiar;

e) apărarea, ordinea publică și securitatea națională;

f) impactul transsectorial sau transfrontalier.

Art. 2 – (1) Entitățile analizează efectul pe care întreruperea, respectiv afectarea confidențialității sau a modului de funcționare a serviciilor pe care le oferă îl poate genera, la nivel național, asupra drepturilor și libertăților fundamentale, asupra economiei naționale, asupra sănătății și vieții persoanelor, în funcție de impactul financiar, precum și asupra apărării, ordinii publice și securității naționale, cât și în funcție de impactul transsectorial sau transfrontalier în relație cu alte state membre ale Uniunii Europeane.

(2) În vederea determinării impactului generat de perturbarea serviciului furnizat de entitate conform dispozițiilor art. 9 lit. b) din Ordonanța de urgență a Guvernului nr. 155/2024, se evaluează nivelul impactului în conformitate cu art. 10 alin. (1) lit. a) - d).

(3) În vederea determinării impactului generat de perturbarea serviciului furnizat de entitate conform art. 9 lit. c) din Ordonanța de urgență a Guvernului nr. 155/2024, se evaluează nivelul impactului în conformitate cu art. 10 alin. (1) lit. f).

(4) În vederea determinării dacă o entitate este considerată esențială în conformitate cu prevederile art. 5 alin. (1) lit. b) din Ordonanța de urgență a Guvernului nr. 155/2024, respectiv dacă este importantă conform prevederilor art. 6 alin. (2) lit. a) din același act normativ, criteriile prevăzute la art. 9 lit. b) și c) din actul normativ menționat anterior se aplică, după caz, astfel:

a) orice entitate din sectoarele din Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 care nu a fost identificată ca entitate esențială conform celorlalte criterii prevăzute la art. 5 din același act normativ, dar care atinge sau depășește pragul ridicat al impactului generat de perturbarea serviciului furnizat, este entitate esențială.

b) orice entitate din sectoarele din Anexele nr. 1 și 2 la Ordonanța de urgență a Guvernului nr. 155/2024 care nu a fost identificată ca entitate importantă conform celorlalte criterii prevăzute la art. 6 din același act normativ sau nu a fost identificată ca entitate esențială conform lit. a), dar care atinge sau depășește pragul mediu al impactului generat de perturbarea serviciului furnizat, este entitate importantă.

Art. 3 – (1) Impactul asupra drepturilor și libertăților fundamentale este ridicat atunci când sunt afectate datele cu caracter personal a mai mult de 1.000.000 de persoane sau este afectat accesul la serviciile publice esențiale pentru un număr de cel puțin 115.000 de persoane.

(2) Impactul asupra drepturilor și libertăților fundamentale este mediu atunci când sunt afectate datele cu caracter personal a mai mult de 200.000 de persoane sau este afectat accesul la serviciile publice esențiale pentru un număr de cel puțin 25.000 de persoane.

Art. 4 – (1) Impactul asupra economiei naționale este ridicat atunci când sunt provocate pierderi de peste 0,1% din PIB-ul României, atunci când este afectată cel puțin 25% din valoarea serviciilor esențiale din unul dintre sectoarele din Anexele nr. 1 și 2 la Ordonanța de urgență a Guvernului nr. 155/2024, sunt provocate distrugeri la nivelul infrastructurii critice, astfel cum acestea sunt prevăzute de Ordonanța de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, cu modificările și completările ulterioare.

(2) Impactul asupra economiei naționale este mediu atunci când este afectată furnizarea serviciilor esențiale din unul dintre sectoarele din Anexele nr. 1 și 2 la Ordonanța de urgență a Guvernului nr. 155/2024, atunci când este afectată funcționarea infrastructurii critice, astfel cum acestea sunt prevăzute de Ordonanța de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, cu modificările și completările ulterioare.

Art. 5 – (1) Impactul asupra sănătății și vieții persoanelor este ridicat atunci când sunt provocate decesul, îmbolnăvirea cronică sau infirmitatea a mai mult de 50 de persoane sau atunci când sunt provocate leziuni traumatice sau este afectată sănătatea a mai mult de 115.000 de persoane.

(2) Impactul asupra sănătății și vieții persoanelor este mediu atunci când sunt provocate leziuni traumatice sau este afectată sănătatea persoanelor.

Art. 6 – (1) Impactul financiar este ridicat atunci când este provocată pierderea a cel puțin 2.500 de lei asupra a cel puțin 115.000 de persoane.

(2) Impactul financiar este mediu atunci când este provocată pierderea a cel puțin 2.500 de lei asupra a cel puțin 25.000 de persoane.

Art. 7 – (1) Impactul asupra apărării, ordinii publice și securității naționale este ridicat atunci când este afectată capacitatea statului de a asigura apărarea, ordinea publică și securitatea națională, precum și generarea incapacității de a îndeplini funcțiile sale principale, sau atunci când este generat un prejudiciu grav asupra reputației statului ori încrederii cetățenilor în acesta.

(2) Impactul asupra apărării, ordinii publice și securității naționale este mediu atunci când este afectată capacitatea statului de a asigura activități din sfera apărării, ordinii publice și securității naționale, cu consecințe potențial grave pentru siguranța persoanelor și a proprietății private.

Art. 8 – (1) Impactul transsectorial sau transfrontalier este ridicat atunci când sunt afectate cel puțin două sectoare și cel puțin 20% dintre serviciile esențiale din cel puțin un sector, sau atunci când obligațiile României ce decurg din dreptul internațional și cadrele multilaterale nu mai pot fi îndeplinite.

(2) Impactul transsectorial sau transfrontalier este mediu atunci când sunt afectate cel puțin două sectoare și cel puțin 5% dintre serviciile esențiale din cel puțin un sector, sau atunci când capacitatea României de a își îndeplini obligațiile ce decurg din dreptul internațional și cadrele multilaterale este afectată.

Anexa nr. 2

Metodologie privind evaluarea nivelului de risc al entităților

Art. 1 - (1) În vederea sprijinirii entităților esențiale și entităților importante, DNSC dezvoltă două mecanisme specifice, respectiv:

a) un instrument de evaluare a nivelului de risc al unei entități – ENIRE@RO;

b) o platformă de înrolare, informare și cooperare – NIS2@RO.

(2) Mecanismele sunt destinate tuturor entităților esențiale și importante înscrise în Registrul entităților, și sunt utilizate în vederea stabilirii nivelului de risc al entității în conformitate cu art. 18 alin. (6) din Ordonanța de urgență a Guvernului nr. 155/2024.

(3) În cazul în care Platforma NIS2@RO este indisponibilă sau se dorește o pre-evaluare a nivelului de risc al unei entități, se utilizează Instrumentul ENIRE@RO, care se descarcă de pe site-urile DNSC (dnsc.ro, platformanis2.ro) și se utilizează local.

Art. 2 - (1) Mecanismele calculează nivelul de risc al entităților din perspectiva a cinci tipologii de actori împărțiți în două grupe, pe baza cunoștințelor și a resurselor pe care le au la dispoziție aceștia, respectiv:

a) cei cu capabilități de nivel comun: teroriști, activiști motivați ideologic și competitori ostili. Aceștia dispun de cunoștințe comune/scăzute și resurse limitate necesare pentru executarea cu succes a unui atac cibernetic;

b) cei cu capabilități extinse: infractori cibernetici și actori statali. Aceștia dispun de cunoștințe avansate și resurse vaste necesare pentru executarea cu succes a unui atac cibernetic.

(2) Pentru calcularea nivelului de risc reprezentat de fiecare categorie de actori, sunt avute în vedere 5 categorii de atacuri cibernetice, în funcție de scopul urmărit și modalitatea de manifestare a amenințării, respectiv:

a) sabotaj/perturbare a furnizării serviciului;

b) furtul de informații/spionaj;

c) atacuri specifice criminalității cibernetice;

d) hacktivism/defacement, dos/ddos;

e) atacuri care țintesc sau care afectează imaginea entității.

Art. 3 - (1) Datele și informațiile utilizate în cele două mecanisme sunt:

a) Date cu valori predefinite la nivel sectorial care nu pot fi modificate:

i. Sectorul evaluat - reprezintă domeniul de activitate al entității analizate. Dacă entitatea activează în mai multe sectoare, nivelul de risc va fi calculat separat pentru fiecare sector, urmând ca măsurile de securitate cibernetică să fie implementate conform celui mai ridicat scor obținut;

ii. Natura atacului - reprezintă modalitatea principală de desfășurare a acestuia, având o valoare prestabilită de către DNSC pentru fiecare sector, astfel: „global” - valoarea ”1” – atacuri nediscriminatorii care vizează cât mai multe dispozitive, servicii sau utilizatori, fără a avea o victimă specifică, și „țintit” - valoarea ”2” – atacuri deliberate asupra unei entități specifice, desfășurate de actori cu expertiză și resurse suficiente, necesitând un grad mai ridicat de protecție.

b) Date care trebuie modificate în conformitate cu dimensiunea entității. În conformitate cu dispozițiile art. 8 din Ordonanța de urgență a Guvernului nr. 155/2024, având în vedere dispozițiile Legii nr. 346/2004 privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cu modificările și completările ulterioare, o entitate poate fi clasificată în:

i. întreprindere mare (L), situație în care acest parametru va avea valoarea ”3”;

ii. întreprindere mijlocie (M), situație în care acest parametru va avea valoarea ”2”;

iii. întreprindere mică și microîntreprindere (S), situație în care acest parametru va avea valoarea ”1”.

În cazul entităților din administrația publică, parametrul va fi calculat în funcție de numărul mediu de persoane angajate, calculat conform dispozițiilor art. 5 din Legea 346/2004, astfel: până la 49 de angajați, va avea valoarea ”1”, între 50 și 249 de angajați va avea valoarea ”2”, minim 250 de angajați, va avea valoarea ”3”.

c) Date cu valori predefinite la nivel sectorial și care pot fi modificate, în mod justificat, de către entitate:

i. Impactul - reprezintă daunele care pot surveni ca urmare a unui atac cibernetic din categoriile prevăzute la dispozițiile art. 2 alin. (2), derulat de un tip de actor prevăzut la dispozițiile art. 2 alin. (1) și este determinat în conformitate cu criteriile și pragurile de determinare a gradului de perturbare a unui serviciu, prevăzute în Anexa nr. 1. Încadrarea în pragurile de impact este raportată la categoria de atac și tipologia de atacator. Această variabilă poate avea următoarele niveluri: „ridicat” - valoare ”10”, „mediu” - valoare ”5” sau „scăzut” - valoare ”0”;

ii. Probabilitatea - reprezintă șansa ca un risc de derulare a unui atac cibernetic din categoriile prevăzute la dispozițiile art. 2 alin. (2), derulat de un tip de actor prevăzut la dispozițiile art. 2 alin. (1), să se materializeze, fiind o măsură a posibilității de apariție a acestuia, determinată fie prin evaluare calitativă, fie prin cuantificare, în funcție de natura riscului și de datele disponibile. Aceasta poate avea următoarele niveluri: „ridicată” - valoarea ”1” – actorul este cunoscut pentru atacuri similare în sectorul respectiv, iar riscul este inacceptabil, necesitând măsuri imediate de reducere sau întreruperea activității; „medie” - valoarea ”0,5” – actorul a desfășurat atacuri similare la nivel global, iar riscul este tolerabil, impunând monitorizare și acțiuni de îmbunătățire pe termen mediu și lung; „scăzută” - valoarea ”0” – nu există dovezi că actorul a efectuat astfel de atacuri în sector, iar riscul este acceptabil fără intervenții suplimentare.

d) Date calculate în mod automat:

i) Valoarea riscului;

ii) Scorul de risc al entității.

(2) Pentru fiecare tip de actor al amenințării, valoarea riscului se calculează în funcție de fiecare categorie de atac cibernetic.

(3) Valoarea riscului se determină prin înmulțirea următorilor parametri: dimensiunea entității, astfel cum aceasta este determinată la dispozițiile alin. (1) lit. b), natura atacului, astfel cum aceasta este determinată la dispozițiile alin. (1) lit. a) pct. ii, impactul, astfel cum acesta este determinat la dispozițiile alin. (1) lit. c) pct. i și probabilitatea, astfel cum aceasta este determinată la dispozițiile alin. (2) lit. c) pct. ii).

Valorile obținute pentru un tip de actor al amenințării, corelat cu fiecare categorie de atac, se adună pentru a determina riscul general asociat respectivului actor al amenințării.

(4) Scorul de risc al entității se determină prin adunarea valorii riscului asociat fiecărui tip de actor al amenințării cu fiecare categorie de atac și este egal cu suma valorilor riscului general pentru toate cele cinci tipuri de actori ai amenințării.

(5) Scorul general al entității va determina nivelul de risc al acesteia în funcție de care se stabilește categoria de cerințe de securitate cibernetică aplicabilă, după cum urmează:

a) entitățile care au obținut un scor între ”0” și ”99” de puncte vor implementa nivelul „Basic”;

b) entitățile care au obținut un scor între ”100” și ”199” de puncte vor implementa nivelul „Important”;

c) entitățile care au obținut un scor între ”200” și ”1.500” de puncte vor implementa nivelul „Esențial”.

(6) În vederea aplicării metodologiei, entitatea înregistrată în Registrul entităților utilizează exclusiv unul dintre cele două mecanisme puse la dispoziție de către DNSC.

Art. 4 – (1) În cazul în care o entitate nu a utilizat Platforma NIS2@RO în cadrul procesului de evaluare a nivelului de risc din cauza indisponibilității acesteia, entitatea va avea obligația de a completa și încărca raportul și documentele justificative, după caz, într-un termen de cel mult 20 de zile de la data la care aceasta devine disponibilă. Validarea și confirmarea acestor acțiuni va fi efectuată de către DNSC.

(2) DNSC recomandă tuturor entităților cărora nu li se aplică prevederile Ordonanței de urgență a Guvernului nr. 155/2024 să implementeze cerințele standardului Cyber Fundamentals, nivel „Basic".

Art. 5 – Se aprobă valorile sectoriale pentru stabilirea nivelului de risc, prevăzute în anexa la prezenta anexă.

Art. 6 – (1) Entitățile din Sectorul 3. Sectorul bancar și entitățile din Sectorul 9. Gestionarea serviciilor TIC (business-to-business) din Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 nu realizează evaluarea nivelului de risc al entității.

(2) Entitățile din Sectorul 3. Sectorul bancar din Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 menționate la alin. (1) aplică măsurile de gestionare a riscurilor în materie de securitate cibernetică astfel cum este prevăzut în *Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011*.

(3) Entitățile din Sectorul 9. Gestionarea serviciilor TIC (business-to-business) din Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 menționate la alin. (1) aplică măsurile de gestionare a riscurilor în materie de securitate cibernetică prevăzute de *Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere.*

(4) Entitățile din Sectorul 4. Infrastructuri ale pieței financiare din Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 cărora li se aplică *Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011*, precum și entitățile din Sectorul 8. Infrastructură digitală din Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024 cărora li se aplică *Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere*, nu realizează evaluarea nivelului de risc al entității.

Valori sectoriale pentru stabilirea nivelului de risc

Risc / Sector		Energie		Transport		Piață financiară		Sănătate		Apă potabilă		Ape uzate		Infrastructură digitală		Administrație publică		Spațiu		Servicii poștale și de curierat		Gestionarea deșeurilor		Fabricarea, producția și distribuția de substanțe chimice		Producția, prelucrarea și distribuția de alimente		Fabricare		Furnizori digitali		Cercetare	
Catogorie atac		Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit	Global	Țintit
terorişti - sabotaj/perturbare a furnizării serviciului	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probabilitate		M		M		M		M		R		R		M		M		M		M		M		M		M		S		M		S
terorişti - furtul de informații/spionaj	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probabilitate		S		S		M		M		M		M		S		M		S		S		M		M		S		S		S		M
terorişti - atacuri specifice criminalității cibernetice	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
terorişti - hacktivism/defacement, dos/ddos	Impact	M		M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
terorişti - atacuri care țintesc sau care afectează imaginea entității	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
activişti motivați ideologic - sabotaj/perturbare a furnizării serviciului	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probabilitate		S		S		M		M		M		M		M		M		S		M		S		S		S		S		M		S
activişti motivați ideologic - furtul de informații/spionaj	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probabilitate		S		S		S		S		S		S		S		S		S		S		M		M		S		S		M		S
activişti motivați ideologic - atacuri specifice criminalității cibernetice	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
activişti motivați ideologic - hacktivism/defacement, dos/ddos	Impact	M		M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probabilitate	M		M		M		S		s		S		M		M		M		S		S		S		M		M		S		M	
	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	

Risc \ Sector		Energie		Transport		Piață financiară		Sănătate		Apă potabilă		Ape uzate		Infrastructură digitală		Administrație publică		Spațiu		Serviciii poștale și de curierat		Gestionarea deșeurilor		Fabricarea, producția și distribuția de substanțe chimice		Producția, prelucrarea și distribuția de alimente		Fabricare		Furnizori digitali		Cercetare	
activiști motivați ideologic - atacuri care țintesc sau care afectează imaginea entității	Probabilitate	M		M		M		M		S		S		M		M		M		M		M		M		M		S		M		S	
competitori ostili - sabotaj/perturbare a furnizării serviciului	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probabilitate		S		S		S		S		S		S		S		S		S		S		S		S		S		M		S		S
competitori ostili - furtul de informații/spionaj	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probabilitate		S		S		S		S		S		S		S		S		S		S		S		S		S		R		S		M
competitori ostili - atacuri specifice criminalității cibernetice	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
competitori ostili - hacktivism/defacement, dos/ddos	Impact	M		M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
competitori ostili - atacuri care țintesc sau care afectează imaginea entității	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
infractori cibernetici - sabotaj/perturbare a furnizării serviciului	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probabilitate		M		S		S		S		S		S		S		M		S		M		S		S		S		S		S		S
infractori cibernetici - furtul de informații/spionaj	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probabilitate		R		R		R		M		M		M		R		R		R		S		M		M		S		M		M		M
infractori cibernetici - atacuri specifice criminalității cibernetice	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probabilitate	R		R		R		R		M		M		R		R		R		R		R		R		M		R		R		R	
infractori cibernetici - hacktivism/defacement, dos/ddos	Impact	M		M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
infractori cibernetici - atacuri care țintesc sau care afectează imaginea entității	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
actori statali - sabotaj/perturbare a furnizării serviciului	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probabilitate		R		R		M		M		R		R		R		R		R		M		M		R		R		M		M		S

Risc \ Sector		Energie		Transport		Piață financiară		Sănătate		Apă potabilă		Ape uzate		Infrastructură digitală		Administrație publică		Spațiu		Serviciii poștale și de curierat		Gestionarea deșeurilor		Fabricarea, producția și distribuția de substanțe chimice		Producția, prelucrarea și distribuția de alimente		Fabricare		Furnizori digitali		Cercetare	
actori statali - furtul de informații/spionaj	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probabilitate		R		R		M		M		M		M		R		R		R		M		M		M		M		M		M		R
actori statali - atacuri specifice criminalității cibernetice	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		M		S		S	
actori statali - hacktivism/defacement, dos/ddos	Impact	M		M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probabilitate	M		M		M		S		S		S		M		M		M		S		S		S		M		S		S		S	
actori statali - atacuri care țintesc sau care afectează imaginea entității	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	
	Probabilitate	S		S		S		S		S		S		S		S		S		S		S		S		S		S		M		M	
Scor standard entitate	mică/micro	95		85		85		72,5		67,5		67,5		95		125		87,5		55		15		60		42,5		57,5		55		62,5	
	mijlocie	190		170		170		145		135		135		190		250		175		110		30		120		85		115		110		125	
	mare	285		255		255		217,5		202,5		202,5		285		375		262,5		165		45		180		127,5		172,5		165		187,5	

Legendă:

Impactul și probabilitatea pot avea următoarele valori, notate în prezentul tabel, după cum urmează:

- Scăzut - S
- Mediu - M
- Ridicat - R