GHID METODOLOGIC PENTRU ELABORAREA PROCEDURII DE MANAGEMENT AL RISCURILOR CIBERNETICE

Aprobat prin Ordinul directorului
Agenției pentru Securitate Cibernetică
Nr. 18 din 21.07.2026

AGENȚIA PENTRU SECURITATE CIBERNETICĂ
+373 681 11 115
WWW.ASC.GOV.MD

Cuprins

Obiectivele managementului riscurilor

Obiectivul principal al managementului riscurilor în cadrul unei organizaţii este identificarea incertitudinilor şi a ameninţărilor care pot afecta atingerea obiectivelor organizaţionale, protejarea organizaţiei împotriva consecinţelor acestora şi facilitarea realizării obiectivelor de bază. Priorităţile managementului riscurilor sunt derivate din obiectivele generale ale organizaţiei, din procesele sale şi din obligaţiile legale şi de reglementare aplicabile. Acestea trebuie stabilite încă din etapa de definire a contextului procesului de management al riscurilor, formulate într-un mod clar şi măsurabil şi corelate cu activele organizaţiei care necesită protecţie împotriva riscurilor şi a efectelor acestora. Pentru monitorizarea gradului de realizare a acestor obiective se recomandă utilizarea indicatorilor-cheie de performanţă (KPI – *Key Performance Indicators*).

În domeniul securităţii cibernetice, aceste principii generale sunt adaptate pentru protejarea activelor informaţionale şi a infrastructurilor digitale. Astfel, obiectivele managementului riscurilor de securitate cibernetică trebuie să fie aliniate cu obiectivele strategice şi operaţionale ale organizaţiei, cu procesele de afaceri, cu cerinţele legale şi de reglementare aplicabile, precum şi cu obligaţiile contractuale privind protecţia informaţiilor şi a serviciilor digitale. Aceste obiective sunt stabilite în etapa de definire a domeniului de aplicare, a contextului şi a criteriilor procesului de management al riscurilor şi trebuie formulate într-un mod clar şi măsurabil, pentru a permite evaluarea eficacităţii măsurilor de securitate implementate.

În acest context, pe lângă indicatorii-cheie de performanţă, organizaţiile utilizează şi indicatori-cheie de risc (KRI – *Key Risk Indicators*), care permit monitorizarea nivelului de expunere la riscurile cibernetice şi a eficacităţii controalelor implementate. Exemple de astfel de indicatori includ nivelul de expunere la vulnerabilităţi, timpul de detectare şi remediere a incidentelor de securitate, numărul incidentelor cibernetice şi gradul de conformitate cu cerinţele de securitate.

Obiectivele managementului riscurilor de securitate cibernetică trebuie să fie corelate cu activele informaţionale, infrastructurile TIC, aplicaţiile, serviciile digitale şi procesele critice ale organizaţiei care necesită protecţie împotriva ameninţărilor cibernetice şi a consecinţelor acestora. Stabilirea acestor obiective constituie fundamentul procesului de identificare, analiză, evaluare şi tratare a riscurilor de securitate cibernetică şi contribuie la reducerea expunerii organizaţiei, asigurarea rezilienţei cibernetice şi atingerea obiectivelor generale ale organizaţiei.

Procesul de management al riscurilor

Procesul de management al riscurilor reprezintă modul specific în care o organizaţie abordează conceptul de risc şi tipurile relevante de riscuri din cadrul său. Acesta constituie o parte fundamentală a oricărei organizaţii şi trebuie integrat în toate procesele şi activităţile relevante şi, dacă este necesar, în funcţie de tipul şi natura activităţii organizaţiei, la mai multe niveluri.

Dacă o organizaţie doreşte să demonstreze conformitatea cu un standard pentru sisteme de management, bazat pe ISO, procesul de management al riscului reprezintă unul dintre procesele fundamentale şi esenţiale din cadrul organizaţiei, în domeniul de aplicare al sistemului de management. Cu toate acestea, ISO 31000:2018 nu oferă îndrumări privind

un sistem de management al riscurilor, ci descrie un cadru de management al riscurilor. Standardul ISO/IEC 27001:2022, fiind un standard pentru sisteme de management bazat pe Cadrul Armonizat, impune existenţa unui proces de management al riscurilor.

Managementul riscurilor poate aborda tipuri individuale de riscuri, precum riscul organizaţional, riscul de piaţă, riscul de credit, riscul operaţional, riscul de proiect, riscul de dezvoltare, riscul lanţului de aprovizionare, riscul infrastructurii, riscurile componentelor sau mai multe dintre aceste categorii ori chiar toate. Această listă nu este exhaustivă, iar în funcţie de specificul activităţii organizaţiei pot exista şi alte tipuri de riscuri relevante.

În cadrul procesului de management al riscurilor, elementele şi principiile generale prevăzute de standardele de referinţă pot fi utilizate pentru a descrie o modalitate de organizare şi implementare a acestui proces în cadrul unei entităţi. Indiferent de abordarea adoptată de fiecare organizaţie, activităţile specifice managementului riscului sunt aplicate într-o măsură variabilă, în funcţie de contextul organizaţional, domeniul de activitate, obiectivele stabilite şi cerinţele aplicabile. Procesul de management al riscurilor poate fi integrat în cadrul diferitelor sisteme de management implementate de organizaţie, contribuind la identificarea, evaluarea, tratarea şi monitorizarea riscurilor asociate activităţilor desfăşurate.

Domeniul de aplicare, contextul şi criteriile

La stabilirea procesului de management al riscurilor în cadrul unei organizaţii, deciziile fundamentale referitoare la procesul de management al riscurilor sunt luate în etapa de definire a domeniului de aplicare, a contextului şi a criteriilor.

În funcţie de domeniul de aplicare al managementului riscului, în cadrul organizaţiei pot fi utilizate diferite subprocese, bazate pe diverse metodologii de evaluare a riscurilor.

Domeniul de aplicare poate fi stabilit pe baza:

- părţilor interesate relevante, atât interne, cât şi externe;
- nivelului de aplicare (strategic, operaţional, la nivel de program, proiect, lanţ de aprovizionare, dezvoltare de produse sau dezvoltare software);
- integrării într-un sistem formal de management;
- relaţiilor cu alte organizaţii, entităţi, activităţi, proiecte sau procese;
- obiectivelor urmărite;
- resurselor disponibile (personal, instrumente software etc.).

Managementul riscurilor în domeniul securităţii cibernetice

Managementul riscurilor aplicat securităţii cibernetice poate viza, de asemenea, diferite domenii de aplicare, cum ar fi:

- infrastructurile critice;
- datele sensibile;
- lanţul de aprovizionare.

În ceea ce priveşte contextul, acesta poate depinde de:

- părţile interesate (interne şi externe);
- obiectivele şi activităţile organizaţiei;
- scopul managementului riscului;

- integrarea într-un cadru existent de management al riscurilor sau într-un sistem de management.

În etapa de stabilire a criteriilor, aflată la începutul implementării managementului riscului, organizaţia, pe baza rezultatelor obţinute în urma definirii domeniului de aplicare şi a contextului, stabileşte şi:

- tipul de risc pe care îl gestionează;
- metodologia de evaluare a riscurilor care va fi aplicată;
- criteriile pentru evaluarea riscurilor;
- criteriile pentru acceptarea riscurilor.

Ulterior, criteriile de risc astfel stabilite au un impact semnificativ asupra activităţilor care urmează în cadrul procesului de management al riscurilor, precum evaluarea riscurilor şi tratarea (mitigarea) riscurilor.

Evaluarea riscurilor

Evaluarea riscurilor este, în mod obişnuit, alcătuită din următoarele etape: identificarea ameninţărilor, evaluarea ameninţărilor, analiza riscurilor şi evaluarea riscurilor.

În funcţie de deciziile luate în etapa de stabilire a domeniului de aplicare, a contextului şi a criteriilor, pot fi implementate metodologii diferite pentru diverse tipuri de riscuri şi pentru diferite niveluri organizaţionale.

Identificarea ameninţărilor reprezintă activitatea de identificare şi descriere sistematică a ameninţărilor şi trebuie să ia în considerare următorii factori:

- sursele de risc;
- cauzele şi evenimentele;
- ameninţările şi vulnerabilităţile;
- riscurile şi ameninţările emergente;
- natura şi valoarea activelor;
- consecinţele şi impactul asupra proceselor şi activelor.

În timpul analizei riscurilor, factorii menţionaţi anterior sunt utilizaţi pentru a înţelege natura şi nivelul unei ameninţări sau al unui risc, pe baza unor elemente precum:

- probabilitatea producerii unui eveniment, a unei ameninţări sau a unui risc;
- amploarea consecinţelor generate de un eveniment, o ameninţare sau un risc;
- complexitatea situaţiei, inclusiv posibilele legături, dependenţe şi efecte în cascadă.

Analiza şi evaluarea riscurilor

În cadrul analizei riscurilor se iau în considerare, de asemenea:

- eficacitatea controalelor (măsurilor de control) existente;
- factorii legaţi de timp, cum ar fi volatilitatea sau perioada analizată.

Rezultatele analizei riscurilor constituie baza pentru evaluarea riscurilor, etapă în care acestea sunt comparate cu criteriile de risc stabilite anterior, inclusiv cu criteriile de acceptare a riscurilor. Aceste rezultate pot fi determinate pe baza criteriilor privind Impactul şi probabilitatea de apariţie, sau prin utilizarea altor metode, precum hărţi de risc (heat maps) sau tabele de evaluare.

Tratarea riscurilor

Tratarea riscurilor reprezintă activitatea de selectare a celei mai adecvate opțiuni pentru gestionarea riscurilor care depășesc nivelul de risc acceptabil stabilit anterior.

Opțiunile de tratare a riscurilor sunt:

- evitarea riscului, prin decizia de a nu începe sau de a nu continua activitatea care generează riscul;
- eliminarea sau reducerea sursei riscului prin:
  - modificarea probabilității de producere a riscului;
  - modificarea impactului și a consecințelor riscului.
- partajarea (transferul) riscului, de exemplu prin contracte sau prin încheierea unor polițe de asigurare;
- acceptarea riscului, în baza unei decizii informate.

Opțiunea de tratare a riscului selectată trebuie să fie aprobată de proprietarul riscului și documentată în mod corespunzător. Pe baza acestei decizii, se elaborează un plan de tratare a riscurilor, care trebuie aprobat și implementat conform planului de proiect inclus în acesta.

Planul de tratare a riscurilor și măsurile de control nou introduse pot genera riscuri sau amenințări noi, care trebuie identificate și gestionate separat.

Utilizarea standardelor în managementul riscurilor

Atunci când integrează conceptul de management al riscurilor în cadrul organizației, o entitate urmărește să adopte abordări adecvate activității sale, precum și domeniului de aplicare și obiectivelor procesului de management al riscurilor.

Organizațiile pot decide că au nevoie de un management integrat al riscurilor la nivel de întreprindere, pentru a gestiona toate tipurile de riscuri (cum ar fi riscurile operaționale, riscurile de piață, riscurile lanțului de aprovizionare, riscurile de proiect sau riscurile strategice), ori doar de gestionarea unui anumit tip de risc (a se vedea exemplele de riscuri menționate anterior).

Pentru aceste domenii de aplicare și obiective diferite și în funcție de activitățile principale ale organizației, pot fi utilizate diverse modele și metodologii de evaluare și tratare a riscurilor.

În acest context, organizațiile pot dori să învețe din experiența altor organizații care activează în același domeniu și să adopte abordări bazate pe bune practici, considerate adecvate atât pentru propria activitate, cât și pentru alte organizații din același sector sau domeniu de activitate.

Pornind de la acest obiectiv, este frecvent întâlnită dezvoltarea unor modele de evaluare sau tratare a riscurilor specifice anumitor sectoare economice sau domenii de activitate, elaborate de asociații profesionale sau grupuri de interes. De multe ori, aceste modele specifice unui sector evoluează în standarde internaționale, prin transmiterea rezultatelor către comitetele tehnice ale organizațiilor internaționale sau europene de standardizare.

Faptul că un astfel de model este recunoscut ca standard de către comunitatea internațională de experți și beneficiază de o utilizare și perfecționare continuă permite

unui număr tot mai mare de organizaţii să identifice soluţii adecvate pentru evaluarea şi tratarea riscurilor.

Aceste standarde pot furniza:

- orientări generale privind terminologia, principiile, modelele de proces şi opţiunile de tratare a riscurilor (de exemplu, ISO 31000);
- descrieri detaliate ale modelelor de evaluare a riscurilor (de exemplu, ISO/IEC 31010 şi ISO/IEC 27005).

Aplicarea acestor standarde la diferite niveluri ale unei organizaţii poate:

- îmbunătăţi reproductibilitatea rezultatelor;
- facilita compararea rezultatelor între organizaţii;
- sprijini evaluarea proceselor de management al riscurilor şi a rezultatelor acestora în cadrul organizaţiei.

De asemenea, utilizarea aceluiaşi standard într-un anumit sector sau domeniu de activitate permite realizarea unor repere, prin compararea performanţei unei organizaţii cu cea a altor organizaţii sau cu media sectorului respectiv.

În principiu, standardele oferă organizaţiilor posibilitatea de a evalua şi compara eficacitatea, eficienţa şi gradul de acoperire al diferitelor modele şi metode utilizate într-un anumit sector sau domeniu de activitate, sprijinind astfel alegerea celui mai potrivit standard pentru integrarea în propriul sistem de management.

Metodologii şi instrumente pentru managementul riscurilor

Obiectivul principal al managementului riscului este, în general, protejarea produselor TIC (software, hardware, sisteme, componente şi servicii), precum şi a activelor organizaţiei, concomitent cu minimizarea costurilor generate de eventualele incidente sau defecţiuni. Prin urmare, managementul riscurilor reprezintă o responsabilitate esenţială pentru succesul activităţilor de afaceri şi al managementului tehnologiei informaţiei. În acest context, el constituie o activitate fundamentală pentru asigurarea securităţii organizaţionale şi se bazează în mod semnificativ pe experienţa acumulată, pe metode consacrate de bune practici şi pe instrumentele utilizate pentru implementarea acestora.

Aceste metode presupun estimarea situaţiei de risc pe baza modelelor proceselor de afaceri şi a infrastructurii existente în cadrul organizaţiei. În acest context, modelele facilitează identificarea riscurilor potenţiale şi dezvoltarea unor măsuri adecvate de protecţie. Accentul principal este pus pe organizaţii şi pe identificarea, analiza şi evaluarea ameninţărilor la adresa activelor şi valorilor acestora.

Rezultatul unei analize de risc constă, de regulă, într-o listă a riscurilor sau ameninţărilor identificate pentru un sistem, împreună cu probabilităţile asociate producerii acestora. Standardele internaţionale din domeniul managementului riscului sunt utilizate pentru a sprijini identificarea acestor riscuri şi ameninţări, precum şi pentru evaluarea probabilităţii lor de apariţie. Aceste standarde acoperă un spectru larg, de la orientări generale privind procesele de management al riscurilor până la ghiduri specifice pentru domeniul tehnologiei informaţiei şi chiar cadre foarte specializate, destinate unor sectoare precum cel maritim. Majoritatea acestor standarde stabilesc condiţiile-cadru ale procesului de management al riscurilor, însă oferă puţine detalii referitoare la metodele concrete de analiză şi evaluare a riscurilor. Din acest motiv, în practică apar frecvent

diferenţe în modul de evaluare a riscurilor în funcţie de domeniul de aplicare, ceea ce face dificilă compararea directă a rezultatelor.

În practică, alegerea metodei şi a instrumentului adecvat pentru analiza şi evaluarea riscurilor este un proces complex. În ultimii ani au fost dezvoltate numeroase concepte, algoritmi şi instrumente rezultate din cercetare, special concepute pentru protejarea infrastructurii TIC şi a sistemelor asociate. Având la bază un context de afaceri, aceste metode utilizează, în general, o evaluare cantitativă a riscurilor fundamentată pe costurile financiare. Exemple relevante sunt metoda EBIOS şi standardul ISO/IEC 27005. În majoritatea acestor metode este utilizată regula empirică bine cunoscută:

Risc = Probabilitate × Impact (Daună potenţială)

În funcţie de metodologia aplicată, termenii utilizaţi şi scalele pentru evaluarea probabilităţii şi a impactului sunt predefinite, aşa cum se întâmplă în metodologia NIST sau în metoda MEHARI.

Pentru a structura procesul de evaluare a riscurilor, au fost dezvoltate diverse abordări bazate pe teoria Bayesiană pentru estimarea probabilităţilor ameninţărilor. De exemplu, metoda OCTAVE utilizează probabilităţi estimate subiectiv, care pot fi interpretate drept distribuţii a priori în cadrul abordării Bayesiene. Această metodă foloseşte UML (Unified Modeling Language) ca limbaj de modelare şi reprezintă o colecţie cuprinzătoa de instrumente şi bune practici pentru managementul riscurilor.

Metoda BowTie este una dintre cele mai utilizate metode calitative de analiză a riscurilor. Metoda CORAS permite integrarea mai multor procese diferite de evaluare a riscurilor, însă probabilitatea producerii unui atac este stabilită înaintea desfăşurării analizei propriu-zise, nefiind determinată automat în cadrul procesului.

Astfel, fiecare organizaţie este responsabilă pentru elaborarea, aprobarea şi implementarea propriei proceduri de management al riscurilor, în conformitate cu metodologia de evaluare a riscurilor selectată şi adaptată specificului activităţilor desfăşurate, domeniului de aplicare şi obiectivelor de securitate stabilite.

Informaţii suplimentare privind standardele, cadrele metodologice şi abordările utilizate în procesul de evaluare a riscurilor sunt disponibile în ghidul ENISA „Risk Management Standards”.

Pentru furnizorii de servicii critice care nu dispun deja de o procedură formalizată de management al riscurilor, este pus la dispoziţie un model orientativ de procedură privind managementul riscurilor, care poate fi utilizat ca punct de referinţă pentru elaborarea şi implementarea propriului proces intern de identificare, evaluare, tratare şi monitorizare a riscurilor de securitate cibernetică.

Modelul are caracter orientativ şi nu limitează utilizarea altor metodologii sau proceduri de management al riscurilor deja implementate de organizaţii, cu condiţia ca acestea să asigure îndeplinirea cerinţelor aplicabile şi să fie adaptate specificului activităţii, profilului de risc şi nivelului de maturitate al organizaţiei.

În completarea acestui model, organizaţiile care nu dispun de un mecanism propriu de evaluare a riscurilor pot utiliza instrumentul online de evaluare a riscurilor https://sirm.asc.gov.md/ care permite completarea structurată a informaţiilor relevante

și transmiterea directă a rezultatelor către autoritatea responsabilă pentru analiză și monitorizare.

Utilizarea modelului de procedură și a instrumentului de evaluare are rol de sprijin metodologic și este doar cu titlu de exemplu pentru furnizori. Acest model nu înlocuiește responsabilitatea organizației de a stabili și menține un proces propriu de management al riscurilor, adecvat cerințelor de securitate cibernetică aplicabile.