RQM CERT
Your Knowledge Provider

GHID ILUSTRAT

MANAGEMENTUL RISCULUI
ȘI TEHNICI DE EVALUARE A RISCULUI

ION IORDACHE

PRECIZĂRI IMPORTANTE!

Deși autorul a acordat toată atenția elaborării acestui Ghid, nu poate fi făcut răspunzător pentru eventualele erori, inclusiv cele cauzate de neglijență. Autorul nu garantează și nu acceptă nicio responsabilitate legală care decurge din, sau în legătură cu acuratețea, fiabilitatea, actualitatea, corectitudinea sau caracterul complet al informațiilor conținute în acest ghid. Dacă, căutați sfaturi cu privire la cerințele dvs. specifice de management al riscurilor, autorul poate acorda consultanță pe bază de contract. Sprijinim și încurajăm diseminarea și schimbul de informații realizând o cercetare rezonabilă pentru a identifica materialele deținute de terți utilizate în informarea din cadrul acestui ghid; referințele utilizate, și alte surse de informare sunt prezentate în Bibliografie.

CUPRINS

Introducere

Organizațiile din toată lumea se confruntă cu un mediu din ce în ce mai dificil și mai complex în care își desfășoare activitățile, fiind obligate la o adaptare permanentă la cerințele clienților lor.

Având în vedere toate aceste evoluții și plecând de la adevărul că riscul este prezent în fiecare aspect al vieții noastre am realizat acest ghid pentru a prezenta elementele de bază ale managementului riscului și pentru a arăta importanța acestuia în succesul sau chiar supraviețuirea unei organizații.

Se depun eforturi permanente pentru a înțelege mai bine riscul și natura acestuia, iar acest lucru a dus la crearea de metodologii și abordări care permit indivizilor și organizațiilor să ia decizii precise, bazate pe raționament logic.

Unul dintre cele mai cunoscute cadre de abordare a riscului este oferit de „**SR ISO 31000:2018 Managementul riscului. Linii directoare**", un standard internațional care încorporează principii, practici dovedite și linii directoare privind gestionarea riscurilor cu care se confruntă organizațiile și care are ca suport standardul „**SR EN IEC 31010:2020 Managementul riscului. Tehnici de evaluare a riscului**".

Ghidul este un preambul la cursul „**Managementul riscului și tehnici de evaluare a riscului**" organizat de RQM Cert, baza pregătirii profesionale pentru certificările internaționale „**PECB Certified ISO 31000 Risk Manager**" și „**PECB Certified ISO 31000 Lead Risk Manager**" despre care găsiți informați complete pe www.rqmcert.com.

Autor,

ION IORDACHE, Ec.

Training & Development Manager, RQM Cert
Consultant de Securitate, iQuality Services

Managementul riscului

„Dacă nu investești în managementul riscului, nu contează în ce afacere te afli, este o afacere riscantă."

(Gary Cohn)

Capacitatea de a gestiona riscul, cantitatea și tipul de riscuri pe care organizațiile acceptă să le urmărească sau să le păstreze pentru a lua decizii cu privirea către viitor, este unul dintre factorii cheie care stimulează dezvoltarea sistemului economic.

Managementul riscului ne ghidează printr-o gamă largă de procese de luare a deciziilor, inclusiv selectarea investițiilor și protejarea vieții și a bunurilor pe care le deținem, sănătatea noastră și multe alte aspecte ale vieții de zi cu zi.

Orice organizație trebuie să includă proceduri adecvate de gestionare a riscurilor care îi afectează operațiunile și activitățile, pentru a gestiona și trata cu succes astfel de riscuri, deoarece riscul este o componentă integrantă a tuturor operațiunilor și activităților comerciale.

Organizațiile de succes sunt cele care sunt capabile să recunoască și să controleze riscurile înainte ca acestea să se materializeze în evenimente distructive care compromit statutul și operațiunile lor.

De regulă, organizațiile recunosc și gestionează riscurile separat, folosind diverse asigurări ca mijloc de a evita incidentele de securitate sau încălcările legale, de exemplu.

S-a dovedit că această abordare este insuficientă, ducând uneori chiar la la o lipsă de coordonare și la scăderea capacității acestora de a recunoaște amenințările strategice.

Prin crearea unei abordări holistice, la nivelul întregii organizații, a managementului riscului, abordare care promovează comunicarea și subliniază pașii esențiali pentru proiectarea și implementarea unui cadru de management al riscului, precum și prin îmbunătățirea continuă a cadrului de management al riscului bazate pe standardul ghid „ISO 31000 Managementul riscului", organizațiile pot îndepărta sau chiar elimina lacunele operaționale create de riscuri

Principii de management al riscului

Scopul managementului riscului este crearea și protejarea valorii. El îmbunătățește performanța, încurajează inovația și sprijină realizarea obiectivelor.

Principiile prezentate în figura de mai jos furnizează îndrumări privind caracteristicile unui management al riscului eficient și eficace, comunicându-i valoarea și explicându-i intenția și scopul.

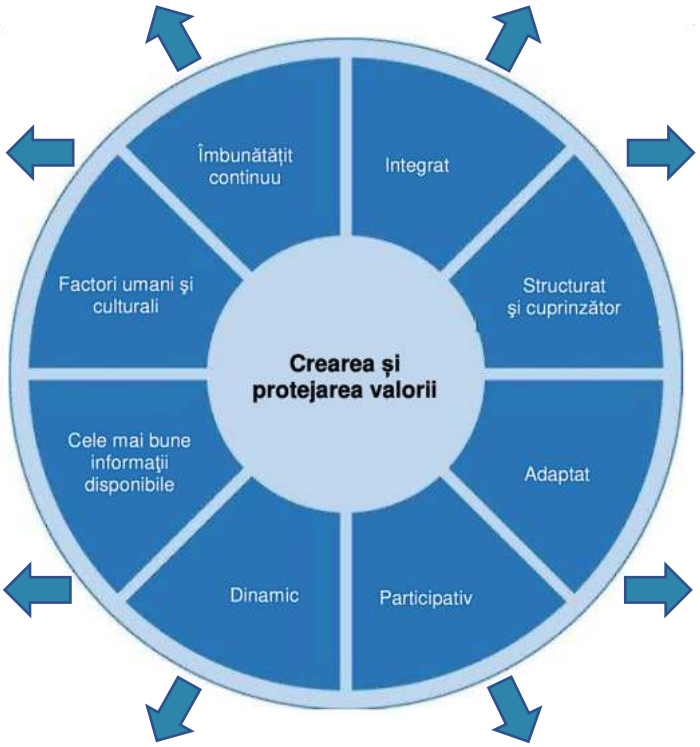
Principiile sunt baza managementului riscului și ar trebui avute în vedere atunci când sunt stabilite cadrul organizațional și procesele managementului riscului în organizație.

Aceste 8 principii din standardul ISO 31000 ar trebui să permită organizației să gestioneze efectele incertitudinii asupra obiectivelor sale.

Managementul riscului este îmbunătățit continuu prin învățare și experiență.

Managementul riscului face parte integrantă din toate activitățile organizației.

Comportamentul uman și cultura influențează în mod managementului riscului la fiecare nivel și în fiecare etapă.



O abordare structurată și cuprinzătoare a managementului riscului contribuie la rezultate consecvente și comparabile.

Elementele de intrare ale managementului riscului se bazează pe informații istorice și informații curente, precum și pe așteptări viitoare.

Cadrul organizațional și procesul de management al riscului sunt adaptate și proporționale cu contextul extern și intern al organizației referitor la obiectivele sale.

Riscurile pot apărea, se pot schimba sau pot dispărea pe măsură ce contextul extern și intern al organizației se schimbă.

Implicarea corespunzătoare și la timp a părților interesate permite luarea în considerare a cunoștințelor, punctelor de vedere și percepțiilor acestora.

CONCLUZIE! Scopul principiilor de management al riscului este de a lega cadrul și practica managementului riscului de obiectivele strategice ale organizației.

Cadru organizational

Scopul unui cadru organizațional al managementului riscului este de a sprijini organizația să integreze managementul riscului în toate activitățile și funcțiile sale semnificative.

Eficacitatea managementului riscului va depinde de integrarea sa în guvernanța organizației, inclusiv în luarea deciziilor. Acest lucru necesită suport din partea părților interesate, în special din partea managementului de la cel mai înalt nivel

Dezvoltarea cadrului organizațional cuprinde integrarea, proiectarea, implementarea, estimarea și îmbunătățirea managementului riscului la nivelul întregii organizații.

Figura prezintă componentele unui cadru organizațional.

Organizația ar trebui să își estimeze practicile și procesele existente de management al riscului, să identifice lacunele și să trateze aceste lacune în interiorul cadrului organizațional.

Componentele cadrului organizațional și modul în care acestea lucrează împreună ar trebui adaptate necesităților organizației.

Top managementul este responsabil juridic pentru raportare referitor la managementul riscului, iar organismele de supraveghere sunt responsabile juridic pentru raportare referitor la supravegherea managementului riscului.

Așa cum se vede din figura de mai sus, pentru a demonstra leadership și angajament, există o serie de responsabilități specifice legate de acțiuni din cadrul sistemului de management al riscului în care top managementul ar trebui sa fie implicat personal.

Adesea, se presupune că organismele de supraveghere trebuie să, sau sunt obligate:

- să se asigure că riscurile sunt luate în considerare în mod corespunzător atunci când stabilesc obiectivele organizației;
- să înțeleagă riscurile cu care se confruntă organizația în efortul său de a-și realiza obiectivele;
- să se asigure că sistemele menite să gestioneze aceste riscuri sunt implementate și funcționează eficace;
- să se asigure că aceste riscuri sunt adecvate în contextul obiectivelor organizației;
- să se asigure că informațiile despre aceste riscuri și managementul lor sunt comunicate în mod adecvat.

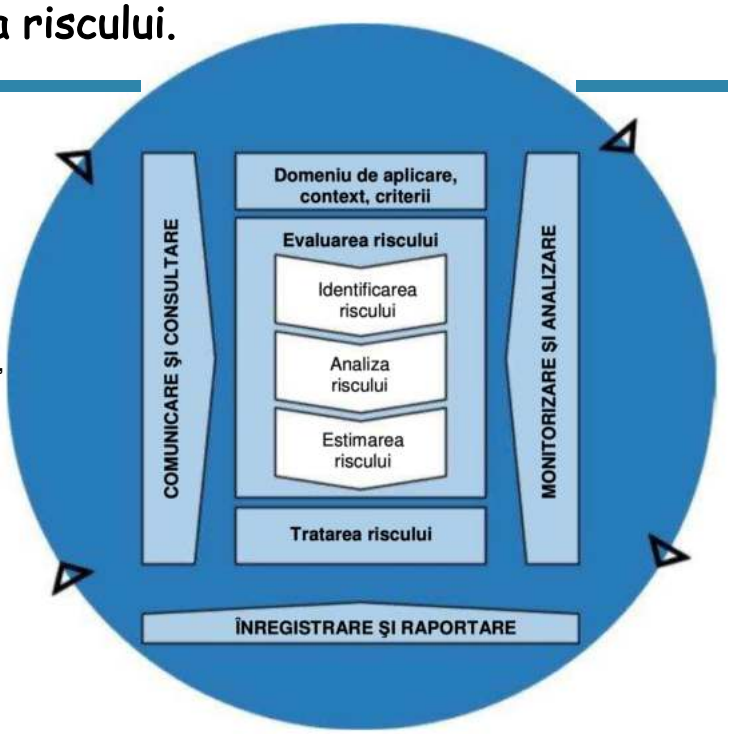
Procesul de management al riscului

Procesul de management al riscului implică aplicarea sistematică a politicilor, procedurilor și practicilor la activitățile de comunicare și consultare, de stabilire a contextului și de evaluare, tratare, monitorizare, analizare, înregistrare și raportare a riscului.

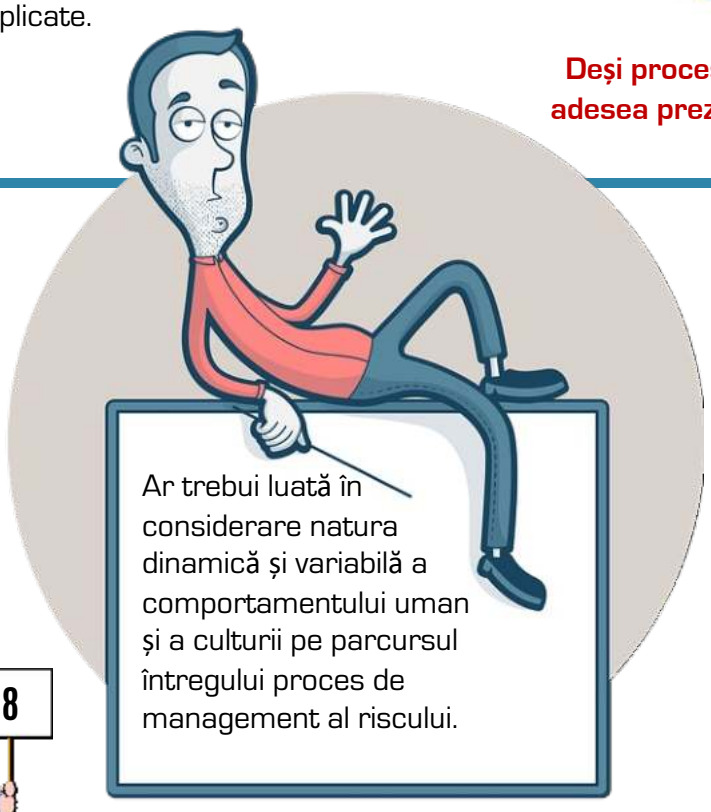
Procesul de management al riscului ar trebui să facă parte integrantă din procesele de management și de luare a deciziilor și să fie integrat în structura, operațiunile și procesele organizației.

Acesta poate fi aplicat la nivel strategic, operațional, al programului sau al proiectului.

Pot exista mai multe moduri de aplicare specifice procesului de management al riscului în cadrul unei organizații, adaptate pentru realizarea obiectivelor și pentru a se potrivi contextului extern și intern în care sunt aplicate.



Deși procesul de management al riscului este adesea prezentat ca fiind secvențial, în practică el este iterativ.

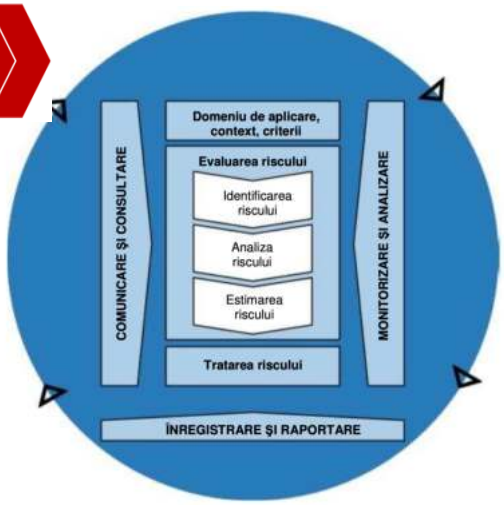


Ar trebui luată în considerare natura dinamică și variabilă a comportamentului uman și a culturii pe parcursul întregului proces de management al riscului.

Scopul comunicării și consultării

este de a ajuta părțile interesate relevante să înțeleagă riscul, baza pe care se iau deciziile și motivele pentru care sunt necesare anumite acțiuni.

Comunicarea caută să promoveze conștientizarea și înțelegerea riscului, în timp ce consultarea implică obținerea feedbackului și a informațiilor care să sprijine procesul de luare a deciziilor.



Domeniu de aplicare, context și criterii

Scopul stabilirii domeniului de aplicare, contextului și criteriilor este adaptarea procesului de management al riscului, permițând o evaluare eficace a riscului și un tratament corespunzător al acestuia.

Domeniul de aplicare, contextul și criteriile implică definirea domeniului de aplicare al procesului și înțelegerea contextului extern și intern.

Atunci când se planifică abordarea, elementele de luat în considerare includ:

- ❑ obiectivele și deciziile necesare;
- ❑ rezultatele așteptate din fiecare etapă a procesului;
- ❑ programarea în timp, amplasamentul, includerile și excluderile specifice;
- ❑ instrumentele și tehnicile adecvate de evaluarea a riscului;
- ❑ resursele necesare, responsabilitățile și înregistrările care vor fi păstrate;
- ❑ relațiile cu alte proiecte, procese și activități.

Organizația ar trebui să definească domeniul de aplicare al activităților sale de management al riscului.

Întrucât procesul de management al riscului poate fi aplicat la diverse niveluri (de exemplu, strategic, operațional, de program, de proiect, sau al altor activități), este important să fie clar domeniul de aplicare avut în vedere, obiectivele relevante care vor fi luate în considerare și alinierea acestora cu obiectivele organizaționale.

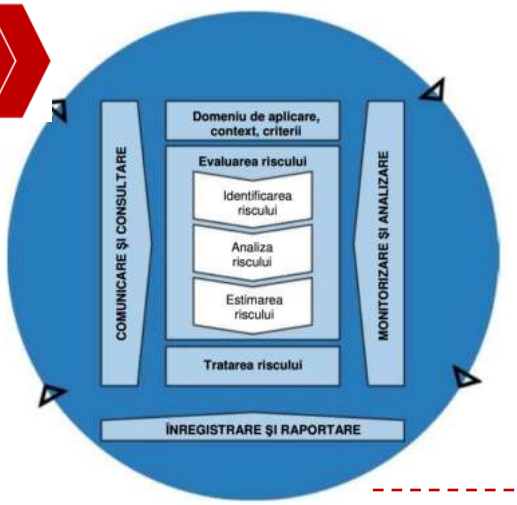
Context extern și intern

Contextul extern și intern este mediul în care organizația dorește să își definească și să își realizeze obiectivele.

Definirea criteriilor de risc

Organizația ar trebui să specifice mărimea și tipul riscului cu care se poate sau nu confrunta, în funcție de obiective. Ar trebui de asemenea să definească criterii pentru estimarea importanței riscului și să sprijine procesele de luare a deciziilor.

Deși se recomandă ca, criteriile de risc să fie stabilite la începutul procesului de evaluare a riscului, aceste criterii sunt dinamice și ar trebui analizate și modificate continuu, dacă este necesar.



Evaluarea riscului

Evaluarea riscului este procesul global de identificare a riscului, analiză a riscului și estimare a riscului.

Evaluarea riscului ar trebui efectuată sistematic, iterativ și prin colaborare, pe baza cunoștințelor și opiniilor părților interesate utilizând cele mai bune informații disponibile, completate cu anchete mai aprofundate dacă este necesar.

Identificarea riscului

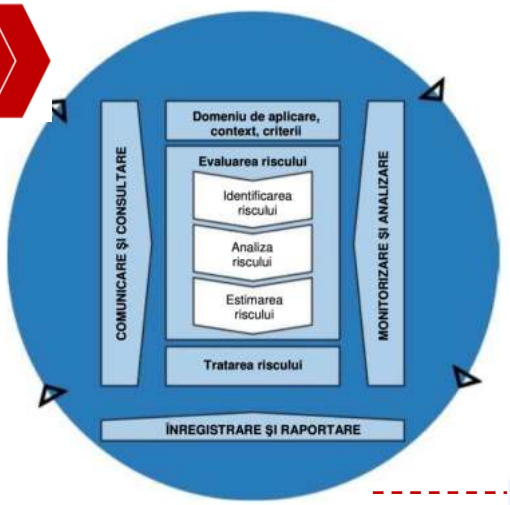
Scopul identificării riscului este de a găsi, recunoaște și descrie riscurile care pot ajuta sau împiedica o organizație să își realizeze obiectivele. Informațiile relevante, adecvate și actualizate sunt importante pentru identificarea riscurilor.

Analiza riscului

Scopul analizei riscului este de a înțelege natura riscului și caracteristicile sale, inclusiv nivelul riscului, atunci când este cazul. Analiza riscului implică luarea în considerare în detaliu a incertitudinilor, a surselor de risc, a consecințelor, plauzibilității, evenimentelor, scenariilor, controalelor și eficacității acestora.

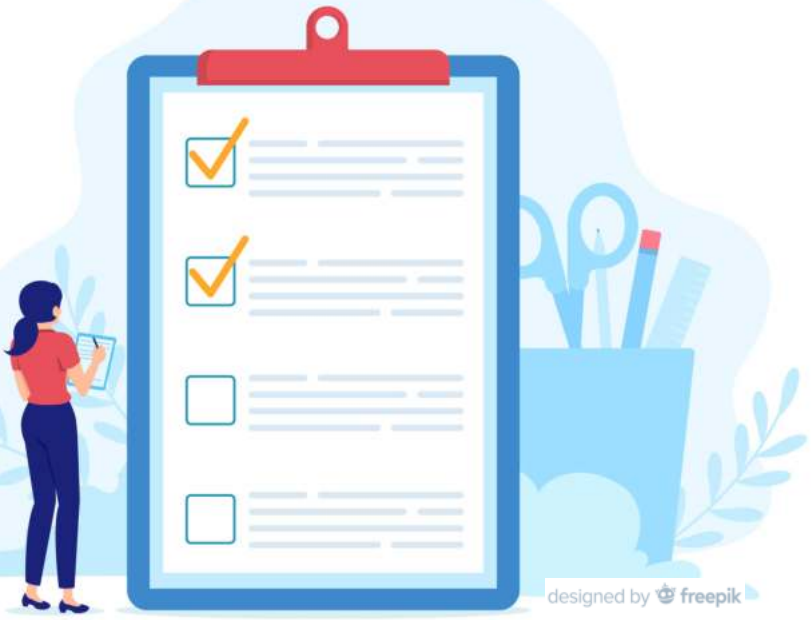
Estimarea riscului

Scopul estimării riscului este de a veni în sprijinul deciziilor. Estimarea riscului implică o comparație între rezultatele analizei riscului și criteriile de risc stabilite, pentru a se determina dacă sunt necesare acțiuni suplimentare.



Tratarea riscului

Scopul tratării riscului este de a selecta și implementa opțiunile de abordare a riscului.



Tratarea riscului implică un proces iterativ de:

- ❑ formulare și selectare a opțiunilor de tratare a riscului;
- ❑ planificare și implementare a tratării riscului;
- ❑ evaluare a eficacității tratării;
- ❑ decizie referitoare la acceptabilitatea riscului rezidual;
- ❑ dacă nu este acceptabil, aplicarea unei tratări suplimentare.

Selectarea opțiunilor de tratare a riscului

Selectarea celei (celor) mai potrivite opțiuni de tratare a riscului implică echilibrarea beneficiilor potențiale legate de realizarea obiectivelor cu costurile, efortul sau dezavantajele implementării.

Opțiunile de tratare a riscului pot implica unul sau mai multe din următoarele elemente:

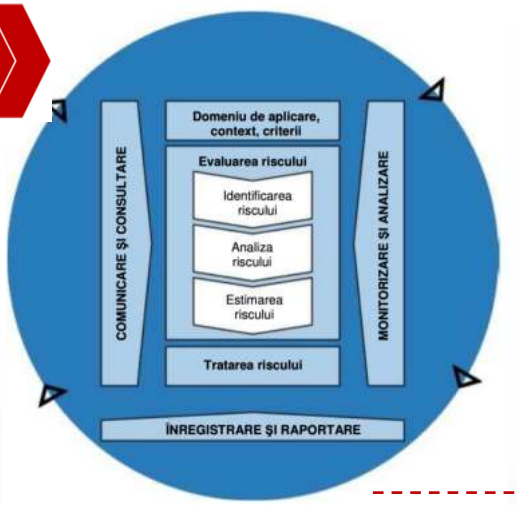
- ❑ evitarea riscului prin decizia de a nu începe sau a nu continua activitatea care generează riscul;
- ❑ asumarea sau creșterea riscului în scopul de a profita de o oportunitate;
- ❑ eliminarea sursei de risc;
- ❑ modificarea plauzibilității;
- ❑ modificarea consecințelor;
- ❑ împărtășirea riscului (de exemplu, prin contracte, prin achiziționarea de asigurări);
- ❑ menținerea riscului prin decizii bazate pe informații.

Elaborarea și implementarea planurilor de tratare a riscului

Scopul planurilor de tratare a riscului este acela de a preciza cum vor fi implementate opțiunile de tratare a riscului selectate, astfel încât dispozițiile acestora să fie înțelese de cei implicați și să poată fi monitorizat progresul față de plan.

Informațiile furnizate de planul de tratare ar trebui să cuprindă:

- ❑ justificarea pentru selectarea opțiunilor de tratare, inclusiv beneficiile așteptate;
- ❑ persoanele responsabile de aprobarea și implementarea planului și care răspund juridic pentru raportare;
- ❑ acțiunile propuse;
- ❑ resursele necesare, inclusiv situațiile neprevăzute;
- ❑ măsurările performanței;
- ❑ constrângerile;
- ❑ raportarea și monitorizarea necesare;
- ❑ programarea în timp a realizării și finalizării acțiunilor.



Monitorizare și analizare Înregistrare și raportare

Scopul monitorizării și analizării este de a se asigura și îmbunătăți calitatea și eficacitatea proiectării, implementării și rezultatelor procesului iar **procesul de management al riscului și rezultatele acestuia** ar trebui documentate și raportate prin mecanisme corespunzătoare.

Monitorizarea continuă și analizarea periodică ale procesului de management al riscului și ale rezultatelor acestuia ar trebui să constituie o componentă planificată a procesului de management al riscului, cu responsabilități clar definite.

Monitorizarea și analizarea ar trebui să aibă loc în toate etapele procesului.

Monitorizarea și analizarea includ planificarea, colectarea și analizarea informațiilor, înregistrarea rezultatelor și furnizarea de feedback.

Rezultatele monitorizării și analizării ar trebui integrate în managementul performanței și în activitățile de măsurare și raportare ale organizației.

Înregistrarea și raportarea au ca scop:

- ❑ comunicarea activităților de management al riscului și a rezultatelor, la nivelul întregii organizații;
- ❑ furnizarea de informații necesare pentru luarea deciziilor;
- ❑ îmbunătățirea activităților de management al riscului;
- ❑ facilitarea interacțiunii cu părțile interesate, inclusiv cu acelea care au responsabilități pentru activitățile de management al riscului și răspund juridic pentru raportare.

Tehnici de evaluare a riscului

„Totul în viață are un anumit risc. Ceea ce trebuie să înveți, de fapt, este cum să navighezi în el."

(Reid Hoffman)

Standardul **„SR EN IEC 31010:2020 Managementul riscului. Tehnici de evaluare a riscului"** oferă îndrumări pentru selectarea și aplicarea diferitelor tehnici care pot fi utilizate pentru a ajuta la îmbunătățirea modului în care incertitudinea este luată în considerare și pentru a ajuta la înțelegerea riscului.

Incertitudine - Termenul incertitudine cuprinde multe concepte subiacente. Tipurile de incertitudine au fost și continuă să fie subiectul a numeroase încercări de clasificare, inclusiv:

- **incertitudine care recunoaște variabilitatea intrinsecă a unor fenomene** și care nu poate fi redusă printr-o cercetare aprofundată (uneori numită incertitudine aleatorie), de exemplu aruncarea unui zar;
- **incertitudine care, de regulă, este rezultatul unei lipse de cunoștințe** și, prin urmare, poate fi redusă prin colectarea mai multor date, rafinarea modelelor, îmbunătățirea tehnicilor de eșantionare etc. (uneori numită incertitudine epistemică).

Risc - Riscul include efectele oricăror forme de incertitudine descrise mai sus. Incertitudinea ar putea conduce la consecințe pozitive sau negative sau ambele.

- **Riscul este adesea descris în termeni de surse de risc, evenimente potențiale, consecințe și plauzibilitate a acestora**. Un eveniment poate avea multiple cauze și poate conduce la consecințe multiple.

Tehnicile de evaluare a riscului urmăresc să ajute oamenii să înțeleagă incertitudinea și riscul asociat în acest context vast, complex și divers, cu scopul de a sprijini decizii și acțiuni mai bine informate.

Utilizarea tehnicilor de evaluare a riscului

Tehnicile descrise în SR EN IEC 31010:2020 oferă o modalitate de a înțelege mai bine incertitudinea și implicațiile sale pentru decizii și acțiuni.

Aplicarea tehnicilor în procesul de management al riscului ISO 31000.

B.1 Tehnici pentru obținerea punctelor de vedere ale părților interesate și experților

- Brainstorming
- Tehnica Delphi
- Tehnica grupului nominal
- Interviuri
- Sondaje

Identificare risc

B.2 Tehnici pentru identificarea riscurilor

- Liste de verificare
- MADE/AMDEC
- HAZOP
- Analiza scenariilor
- SWIFT

B.3 Determinare surse, cauze și factori dominanți ai riscului

- Abordare cindynică
- Metoda Ishikawa
- Analiza cauzei rădăcină

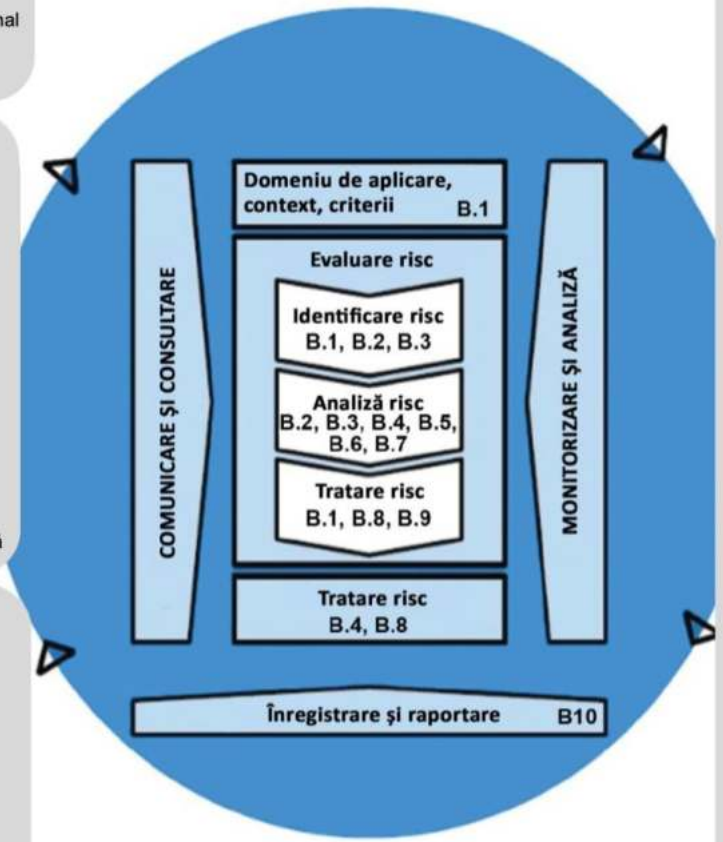
Estimare risc

B.8 Tehnici de estimare a importanței riscului

- ALARP/SFAIRP
- Diagrame număr-frecvență (F-N)
- Diagrame Pareto
- Mentenanța bazată pe fiabilitate
- Indici de risc

B.3 Tehnici de selectare dintre opțiuni

- Analiza cost/beneficiu
- Analiza arbore de decizie
- Teoria jocului
- Analiza multi-criterii



B.10 Tehnici pentru înregistrare și raportare

- Registru de riscuri
- Matrice consecință-plauzibilitate
- Curbe S
- Papion

Analiză risc

B.4 Tehnici pentru analiza controalelor

- Analiza papion
- HACCP
- LOPA

B.5 Tehnici pentru înțelegerea consecințelor și plauzibilității

- Analiza bayesiană
- Rețele Bayesiene
- Analiza de impact asupra afacerii
- Analiza arbore de evenimente
- Analiza arbore de defectare
- Analiza cauză-consecință
- Analiza Markov
- Simularea Monte Carlo

B.6 Tehnici pentru analiza interdependențelor

- Harta cauzală
- Analiza impactului încrucișat

B.7 Tehnici care oferă o măsură a riscului

- Evaluarea riscului toxicologic
- Analiza impactului protecției datelor
- Valoarea la risc (VaR)
- Valoarea condiționată la risc

IEC

Modul în care este evaluat riscul depinde de complexitatea și noutatea situației, precum și de nivelul relevant de cunoștințe și de înțelegere.

Implementarea evaluării riscului

O evaluare a riscului de securitate este un element important în procesul general de management al riscului de securitate. Conform SR EN IEC 31010:2020 există șase etape ale implementării evaluării riscului.

1

Planificarea evaluării

Ar trebui stabilit scopul evaluării, inclusiv identificarea deciziilor sau a acțiunilor la care se referă, a factorilor de decizie, a părților interesate, a calendarului și a naturii elementului de ieșire cerut (de exemplu, dacă sunt solicitate informații calitative, semicantitative sau cantitative).

2

Gestionarea informațiilor și dezvoltarea de modele

Înainte și în timpul unei evaluări a riscului, ar trebui obținute informații relevante. Aceste informații oferă elemente de intrare pentru analiza statistică, modelele sau tehnicile descrise n capitolul următor. În unele cazuri, informațiile pot fi utilizate de factorii de decizie fără o analiză suplimentară.

3

Aplicarea tehnicilor de evaluare a riscurilor

Tehnicile descrise în capitolul următor sunt utilizate pentru a dezvolta o înțelegere a riscului ca element de intrare în deciziile în care există incertitudine, inclusiv în deciziile referitoare la dacă și cum să fie tratat riscul.

4

Examinarea analizelor

Atunci când este posibil, rezultatele analizelor ar trebui verificate și validate. Verificarea implică confirmarea că analiza a fost făcută corect. Validarea implică verificarea că a fost realizată analiza corectă pentru a obține obiectivele cerute. În unele situații, verificarea și validarea pot implica procese independente de examinare.

5

Aplicarea rezultatelor pentru a sprijini deciziile

Rezultatele analizei riscului furnizează un element de intrare pentru deciziile necesar a fi luate și acțiunile întreprinse.

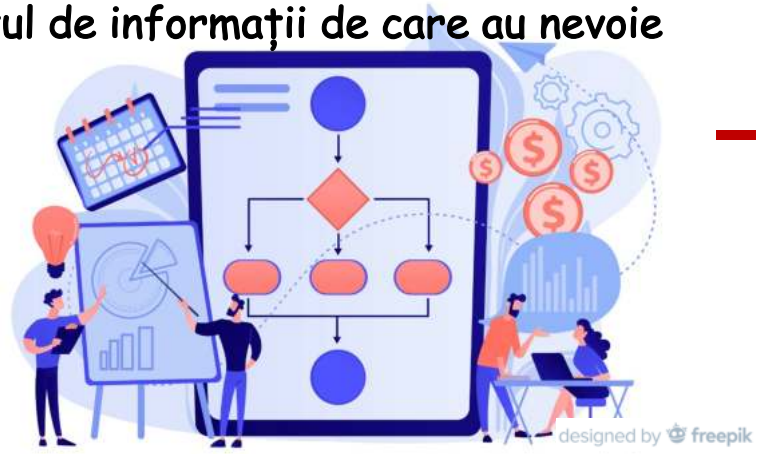
6

Înregistrare și raportare a procesului de evaluare a riscului și a rezultatelor acestuia

Rezultatele evaluării riscului, metodologiile utilizate, justificarea ipotezelor și a oricăror recomandări ar trebui să fie documentate și să se ia o decizie referitoare la ce informații este necesar să fie comunicate și cui. Ar trebui definit modul în care înregistrările urmează să fie analizate și actualizate.

Selectarea tehnicilor de evaluare a riscului

Alegerea tehnicii și modul în care aceasta este aplicată ar trebui adaptate contextului și utilizării și ar trebui să furnizeze tipul și formatul de informații de care au nevoie părțile interesate.



În termeni generali, numărul și tipul de tehnici selectate ar trebui adaptate în funcție de importanța deciziei și ar trebui să țină cont de constrângerile de timp, de alte resurse, precum și de costurile de oportunitate.

Unele dintre tehnicile descrise în acest document pot fi aplicate în timpul etapelor procesului de management al riscului din ISO 31000, în plus față de utilizarea lor în evaluarea riscului.

Este adesea posibil să se aleagă tehnicile relevante pentru o anumită circumstanță iar la selectarea unei tehnici sau a mai multor tehnici ar trebui luate în considerare următoarele:

- ❑ scopul evaluării;
- ❑ necesitățile părților interesate;
- ❑ orice cerințe legale, reglementate și contractuale;
- ❑ mediul de operare și scenariul;
- ❑ importanța deciziei (de exemplu, consecințele în cazul în care se ia o decizie greșită);
- ❑ orice criterii de decizie definite și forma acestora;
- ❑ timpul disponibil înainte de luarea unei decizii;
- ❑ informațiile disponibile sau care pot fi obținute;
- ❑ complexitatea situației;
- ❑ expertiza disponibilă sau care poate fi obținută.

Capitolul următor conține scurte prezentări generale a șapte tehnici de evaluare a riscurilor, utilizarea fiecăreia, elementele de intrare și de ieșire, punctele tari și limitările lor.

Aceste tehnici sunt detaliate, cu studii de caz pentru fiecare, în cursul „Managementul Riscului și Tehnici de Evaluare a Riscului" organizat de RQM Cert. (www.rqmcert.com)

Brainstorming

Brainstormingul este un proces folosit pentru a stimula și încuraja un grup de oameni să dezvolte idei legate de unul sau mai multe subiecte de orice natură.

Termenul „brainstorming" este adesea folosit pentru a desemna orice tip de discuție de grup, dar brainstormingul eficace necesită un efort conștient pentru a se asigura că gândurile celorlalți din grup sunt utilizate ca instrumente pentru a stimula creativitatea fiecărui participant. **Orice analiză sau critică a ideilor se realizează separat de brainstorming.**

Mod de utilizare

Brainstormingul poate fi aplicat la orice nivel într-o organizație pentru a identifica incertitudini, moduri de succes sau eșec, cauze, consecințe, criterii pentru decizii sau opțiuni de tratare.

Utilizarea cantitativă este posibilă, dar numai în forma sa structurată, pentru a se asigura că preferințele sunt luate în considerare și sunt tratate, mai ales atunci când sunt implicate pe toate părțile interesate.

Elemente de intrare/ieșire

Brainstormingul evidențiază punctele de vedere ale participanților, astfel încât are mai puțină nevoie de date sau informații externe decât alte metode. Este necesar ca printre participanți să existe persoane cu expertiză, experiență și puncte de vedere diferite, pentru problema în cauză.

Elementele de ieșire sunt sub forma unei liste a tuturor ideilor generate în timpul sesiunii și a gândurilor formulate la prezentarea ideilor.

Puncte tari și limitări

Punctele tari ale brainstorming-ului includ următoarele:

- ❑ încurajează imaginația și creativitatea, ceea ce ajută la identificarea de noi riscuri și noi soluții;
- ❑ este util acolo unde există date puține sau deloc și unde sunt necesare tehnologii sau soluții noi;
- ❑ implică părțile interesate cheie și, prin urmare, ajută la comunicare și angajare;
- ❑ este relativ rapid și ușor de configurat.

Limitările includ următoarele:

- ❑ este dificil de demonstrat că procesul a fost cuprinzător;
- ❑ grupurile tind să genereze mai puține idei decât persoanele care lucrează singure;
- ❑ o anumită dinamică de grup ar putea însemna că unele persoane cu idei valoroase rămân tăcute, în timp ce altele domină discuția. Acest lucru poate fi depășit printr-o facilitare eficace;
- ❑ încurajarea gândirii creative și a ideilor noi poate însemna faptul că discuția nu rămâne concentrată asupra problemei luată în considerare și consumă din timpul alocat întâlnirii.

Interviuri structurate sau semi-structurate

Într-un interviu structurat, persoanelor intervievate li se adresează un set de întrebări pregătite anterior.

Un interviu semi-structurat este similar, dar se lasă mai multă libertate ca, prin conversație, să se exploreze aspectele care apar.

Mod de utilizare

Interviurile structurate și semi-structurate sunt un mijloc de a obține informații și opinii aprofundate de la persoanele dintr-un grup.

Dacă este necesar, răspunsurile lor pot fi confidențiale.

Acestea furnizează informații aprofundate în cazul în care persoanele nu sunt influențate de punctele de vedere ale altor membri dintr-un grup.

Acestea sunt utile dacă este dificil ca participanții să fie reuniți în același loc simultan sau dacă discuția liberă într-un grup nu este adecvată situației sau persoanelor implicate.

Elemente de intrare/ieșire

Elementele de intrare sunt: o înțelegere clară a informațiilor necesare și un set de întrebări pregătite anterior care au fost testate cu un grup pilot.

Este necesar ca cei care concep interviul și cei care pun întrebările să aibă unele abilități pentru a obține răspunsuri bune, valide și care nu sunt influențate de propriile prejudecăți.

Elementele de ieșire sunt informațiile detaliate cerute.

Puncte tari și limitări

Punctele tari ale interviurilor structurate includ următoarele:

lasă persoanelor timp să reflecteze la un anumit aspect;

comunicarea unu-la-unu poate permite o considerare mai aprofundată a aspectelor decât o abordare de grup;

interviurile structurate permit implicarea unui număr mai mare de părți interesate decât un grup față în față.

Limitările includ următoarele:

- ❑ interviurile consumă mult timp pentru concepție, realizare și analiză;
- ❑ au nevoie de o anumită expertiză pentru concepție și realizare, dacă răspunsurile trebuie să nu fie influențate de către cel care ia interviul;
- ❑ părerile preconcepute din răspunsuri sunt tolerate, ele nu sunt nici moderate, nici eliminate prin discuții de grup;
- ❑ interviurile nu stimulează imaginația (care este o caracteristică a metodelor de grup);
- ❑ interviurile semi-structurate produc o cantitate considerabilă de informații exprimate cu cuvintele celui intervievat.

Sondaje

În general, sondajele implică mai mulți oameni decât interviurile și, de obicei, pun întrebări mai precise.

De obicei, un sondaj va implica un chestionar pe calculator sau pe hârtie.

Întrebările oferă adesea răspunsuri de tip da/nu, alegere dintr-o scară de evaluare sau alegere dintr-o serie de opțiuni.

Mod de utilizare

Sondajele pot fi utilizate în orice situație în care este utilă consultarea largă a părților interesate, în special atunci când este nevoie de informații relativ puține de la un număr mare de persoane.

Elemente de intrare/ieșire

Întrebări verificate în prealabil, lipsite de ambiguitate, trimise unui eșantion larg reprezentativ de persoane care doresc să participe. Este necesar ca numărul de răspunsuri să fie suficient pentru a oferi validitate statistică.

Rezultatul este o analiză a punctelor de vedere de la mai multe persoane, adesea sub formă grafică.

Puncte tari și limitări

Punctele tari ale sondajelor includ următoarele:

- ❑ poate fi implicat un număr mai mare de participanți decât pentru interviuri, oferind informații mai bune într-un grup;
- ❑ derularea sondajelor are un cost relativ redus, mai ales dacă se utilizează software online capabil să furnizeze unele analize statistice;
- ❑ pot furniza informații valabile din punct de vedere statistic;
- ❑ rezultatele sunt ușor de pus sub formă de tabel și ușor de înțeles: de obicei este posibilă reprezentarea grafică;
- ❑ rapoartele sondajelor pot fi puse la dispoziția altora relativ ușor.

Limitările includ următoarele:

- ❑ natura întrebărilor este limitată de necesitatea de a fi simple și fără ambiguități;
- ❑ de obicei, este necesar să se obțină unele informații demografice pentru a interpreta rezultatele;
- ❑ numărul de întrebări care pot fi incluse este limitat dacă se așteaptă un număr suficient de răspunsuri;
- ❑ persoana care pune întrebarea nu poate să o explice, astfel încât respondenții ar putea interpreta întrebarea în mod diferit decât a fost intenționat;
- ❑ este dificil să fie concepute întrebări care să nu-i conducă pe respondenți la anumite răspunsuri;
- ❑ chestionarele tind să aibă la bază ipoteze care ar putea să nu fie valabile.

Liste de verificare

Listele de verificare sunt utilizate în timpul evaluării riscului în diferite moduri, cum ar fi pentru a ajuta la înțelegerea contextului, la identificarea riscului și la gruparea riscurilor în diferite scopuri în timpul analizei.

O listă de verificare se poate baza pe experiența eșecurilor și succeselor din trecut dar, într-o manieră mai formală, pot fi dezvoltate tipologii de risc și taxonomii pentru a categorisi sau a clasifica riscurile pe baza atributelor comune.

Mod de utilizare

Listele de verificare pot fi concepute pentru a se aplica la nivel strategic sau operațional.

Acestea pot fi aplicate folosind chestionare, interviuri, workshopuri structurate sau combinații ale celor trei, în metode față în față sau care se bazează pe calculator.

Exemplu de liste de verificare, utilizate, de regulă, la nivel strategic:

SWOT (strengths, weaknesses, opportunities and threats - puncte tari, puncte slabe, oportunități și amenințări) identifică factorii din contextul intern și extern pentru a ajuta la stabilirea obiectivelor și a strategiilor de realizare a acestora, ținând cont de risc.

La nivel operațional, sunt utilizate listele de verificare a pericolelor pentru a identifica pericolele și pentru a efectua analiza preliminară a pericolelor.

Acestea sunt evaluări preliminare ale riscurilor de securitate, efectuate de obicei în etapa inițială de concepere a unui proiect.

În general, cu cât lista de verificare este mai specifică, cu atât este mai limitată utilizarea sa la contextul particular în care este dezvoltată.

Elemente de intrare/ieșire

Elementele de intrare sunt date sau modele din care să se dezvolte liste de verificare, taxonomii sau clasificări valide.

Elementele de ieșire sunt liste de verificare, întrebări sau categorii și scheme de clasificare.

Puncte tari și limitări

Punctele tari ale listelor de verificare:

- ❑ promovează o înțelegere comună a riscului, între părțile interesate;
- ❑ atunci când sunt bine concepute, aduc o experiență largă într-un sistem ușor de utilizat pentru cei care nu sunt experți;
- ❑ odată dezvoltate, necesită puțină expertiză specializată.

Limitările listelor de verificare:

- ❑ utilizarea este limitată în situații noi în care nu există istoric relevant sau în situații care diferă de cea pentru care au fost dezvoltate;
- ❑ tratează situațiile deja cunoscute sau imaginate;
- ❑ lipsa informațiilor poate duce la suprapuneri și/sau lacune (de exemplu, schemele nu se exclud reciproc și nu sunt exhaustive);
- ❑ pot încuraja tipul de comportament „bifați căsuța” mai degrabă decât explorarea ideilor.

Tehnica Delphi

Tehnica Delphi este o procedură pentru obținerea consensului de opinie de la un grup de experți.

„Tehnica Delphi poate fi caracterizată ca o metodă de structurare a unui proces de comunicare de grup, astfel încât procesul să fie eficient pentru a permite unui grup de indivizi, în ansamblu, să se ocupe de o problemă complexă."

(The Delphi Method: Techniques and Applications)

O caracteristică esențială a tehnicii Delphi este că experții își exprimă opiniile în mod individual, independent și anonim, în timp ce au acces la punctele de vedere ale celorlalți experți pe măsură ce procesul avansează.

Fiecare expert primește un rezumat al rezultatelor rundei anterioare de sondaje după fiecare rundă, permițându-i să-și modifice răspunsurile în lumina consensului.

Mod de utilizare

Tehnica Delphi este utilizată pentru probleme complexe la care există incertitudini și pentru care este necesar un raționament al unui expert pentru a face față acestor incertitudini.

Poate fi utilizată în prognoze, în elaborarea de politici și pentru a obține consens sau pentru a concilia diferențele dintre experți.

Poate fi folosită pentru a identifica riscurile, amenințările și oportunitățile și pentru a obține un consens referitor la plauzibilitatea și consecințele evenimentelor viitoare.

Elemente de intrare/ieșire

Metoda se bazează pe cunoștințele și cooperarea continuă a participanților, într-o perioadă de timp variabilă care poate fi de zile, săptămâni, luni sau chiar ani.

Elemente de ieșire: consens asupra subiectului luat în considerare.

Puncte tari și limitări

Punctele tari includ următoarele:

- ❑ întrucât punctele de vedere sunt anonime, este mai probabil ca opiniile nepopulare să fie exprimate și există o mai mică influență cauzată de ierarhie;
- ❑ toate punctele de vedere au aceeași pondere, ceea ce evită problema personalităților dominante;
- ❑ obține proprietatea asupra rezultatelor;
- ❑ nu este necesar ca participanții să fie adunați în același loc, în același timp;
- ❑ participanții au timp să pregătească atent răspunsul la întrebări;
- ❑ procesul presupune că experții își dedică toată atenția sarcinii.

Limitările includ următoarele:

- ❑ necesită mult timp și efort,
- ❑ este necesar ca participanții să fie capabili să se exprime clar în scris.

Analiza cost beneficiu

Analiza cost/beneficiu stabilește ponderea costurilor totale preconizate ale opțiunilor în termeni monetari față de beneficiile totale preconizate, pentru a alege opțiunea cea mai profitabilă sau cea mai eficace.

Analiza cost/beneficiu poate fi calitativă sau cantitativă sau poate combina elemente cantitative și calitative și poate fi aplicată la orice nivel al unei organizații.

Părțile interesate care ar putea suporta costuri sau ar putea primi beneficii (tangibile sau intangibile) sunt identificate împreună cu beneficiile și costurile directe și indirecte pentru fiecare dintre acestea.

Costurile directe sunt costurile direct asociate cu acțiunea. **Costurile indirecte** sunt costurile suplimentare de oportunitate, cum ar fi scăderea utilității, consumarea din timpul alocat managementului sau devierea capitalului de la alte investiții potențiale.

Mod de utilizare

Analiza cost/beneficiu este utilizată la niveluri operațional și strategic pentru a ajuta la alegerea dintre mai multe opțiuni. În cele mai multe cazuri, aceste opțiuni vor implica incertitudine. În calcule trebuie luate în considerare atât variabilitatea valorii actuale preconizate a costurilor și beneficiilor, cât și posibilitatea unor evenimente neprevăzute.

Elemente de intrare/ieșire

Elementele de intrare includ informații despre costuri și beneficii pentru părțile interesate relevante și despre incertitudinile legate de aceste costuri și beneficii. **Elementele de ieșire** ale unei analize cost-beneficiu sunt informații despre costurile și beneficiile în funcție de diferite opțiuni sau acțiuni.

Puncte tari și limitări

Puncte tari ale analizei cost/beneficiu: permite compararea costurilor și beneficiilor în funcție de un singur metric (de obicei în bani); asigură transparența informațiilor utilizate pentru luarea de decizii și încurajează colectarea de informații detaliate despre toate aspectele posibile ale unei decizii (acestea pot fi valoroase pentru dezvăluirea aspectelor ignorate și pentru comunicarea cunoștințelor).

Limitările includ următoarele: necesită o bună înțelegere a beneficiilor plauzibile, astfel încât nu este adecvată unei situații noi, cu un nivel ridicat de incertitudine; analiza cantitativă poate produce cifre semnificativ diferite în funcție de ipotezele și metodele utilizate pentru a atribui valori economice beneficiilor neeconomice și intangibile iar pentru unele aplicații, este dificil a se defini o rată de actualizare valabilă pentru costurile și beneficiile viitoare; nu tratează bine incertitudinea referitoare la momentul apariției costurilor și beneficiilor sau flexibilitatea în luarea deciziilor viitoare.

Analiza impactului asupra vieții private (PIA)

PIA - Privacy Impact Analysis

DPIA - Data Protection Impact Analysis

Metodele de analiză a impactului asupra confidențialității (PIA) (cunoscută și sub denumirea de evaluarea impactului asupra confidențialității) și analiză a impactului asupra protecției datelor (DPIA) analizează modul în care incidentele și evenimentele ar putea afecta viața privată a unei persoane (PI) și identifică și cuantifică capacitățile care ar fi necesare pentru gestionarea acesteia.

O analiza PIA/DPIA este un proces de evaluare a unei propuneri de identificare a efectelor potențiale asupra vieții private și datelor cu caracter personal.

Mod de utilizare

O analiză PIA/DPIA este utilizată pentru a determina consecințele riscurilor ridicate aferente proceselor și resurselor asociate (de exemplu, persoane, echipamente și tehnologie informațională), pentru a limita consecințele negative potențiale asupra vieții private a persoanelor care rezultă din modul în care sunt tratate informațiile.

Elemente de intrare/ieșire

Elementele de intrare includ:

- ❑ informații referitoare la obiectivele, direcția strategică, mediul, activele și interdependențele organizației.
- ❑ o evaluare a priorităților în urma examinării anterioare a riscurilor de bază;
- ❑ un chestionar pregătit sau alte mijloace de colectare a informațiilor.

Elementele de ieșire includ:

- ❑ documente care detaliază informațiile colectate ca elemente de intrare.

Puncte tari și limitări

Puncte tari:

- ❑ o înțelegere profundă a proceselor critice care tratează informații personale (sensibile) în cadrul sau în numele unei organizații;
- ❑ evaluarea implementării conceptului de viață privată încă din etapa de proiectare și prin aplicarea de principiile implicite;
- ❑ înțelegerea resurselor-cheie necesare în cazul unei scurgeri sau pierderi de date cu caracter personal;
- ❑ informațiile necesare pentru planificarea răspunsului unei organizații în cazul unui incident referitor la datele cu caracter personal.

Limitări:

- ❑ în faza inițială (examinarea impactului asupra vieții private) poate exista un calcul simplist sau subestimat al severității potențiale a riscului pentru viața privată a unei persoane;
- ❑ poate fi dificil să se obțină un nivel adecvat de înțelegere a operațiunilor și activităților organizației atunci când sunt prelucrate date cu caracter personal.

RQM CERT
Your Knowledge Provider

www.rqmcert.com

PECB BEYOND RECOGNITION

PECB Certified ISO 31000
Risk Manager

Learn to help organizations establish a risk management framework and apply the risk management process based on ISO 31000

Why should you take this training course?

Risks come from multiple sources and can appear in many shapes and sizes. Almost every strategic decision within an organization is accompanied by certain risks that the organization must acknowledge and deal with. Since without taking risks, there is virtually no growth, risk management should be an integral part of the processes in every organization.

The ISO 31000 Risk Manager training course helps participants acquire the knowledge necessary and ability to integrate the risk management guidelines of ISO 31000 in an organization. It provides information with regard to the risk management principles and their application, as well as the core elements of the risk management framework and steps for a risk management process. In addition, it provides the basic approaches, methods, and practices for assessing risk in a wide range of situations.

PECB AUTHORIZED PARTNER PECB GOLD PARTNER

RQM CERT Your Knowledge Provider

www.rqmcert.com

PECB BEYOND RECOGNITION

PECB Certified ISO 31000
Lead Risk Manager

Obtain the necessary competencies to guide and support organizations establish a risk management framework based on ISO 31000 and other best practices and recommendations for risk management

Why should you attend?

The ISO 31000 Lead Risk Manager training course helps participants develop their competences to support an organization create and protect value by managing risks, making decisions, and improving performance using the ISO 31000 guidelines. It provides information regarding the core elements and the effective implementation of a risk management framework, the application of the risk management process, and the actions necessary for the successful integration of these elements to meet organizational objectives. Furthermore, it provides guidance on the selection and application of techniques for assessing risks in a wide range of situations.

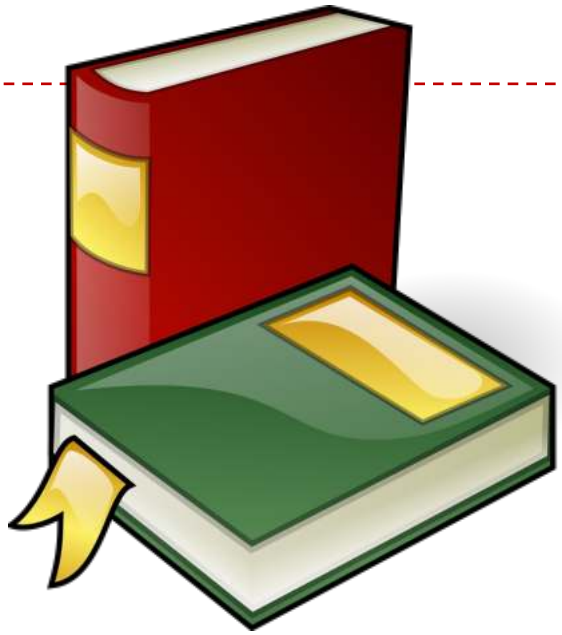
Upon completion of the training course, participants can sit for the exam and apply to obtain the "PECB Certified ISO 31000 Lead Risk Manager" credential. The credential demonstrates that the participant possesses the theoretical and practical knowledge and professional capabilities to support and lead risk management processes based on ISO 31000 guidelines and best practices in this field.

PECB AUTHORIZED PARTNER PECB GOLD PARTNER

RQM CERT Your Knowledge Provider

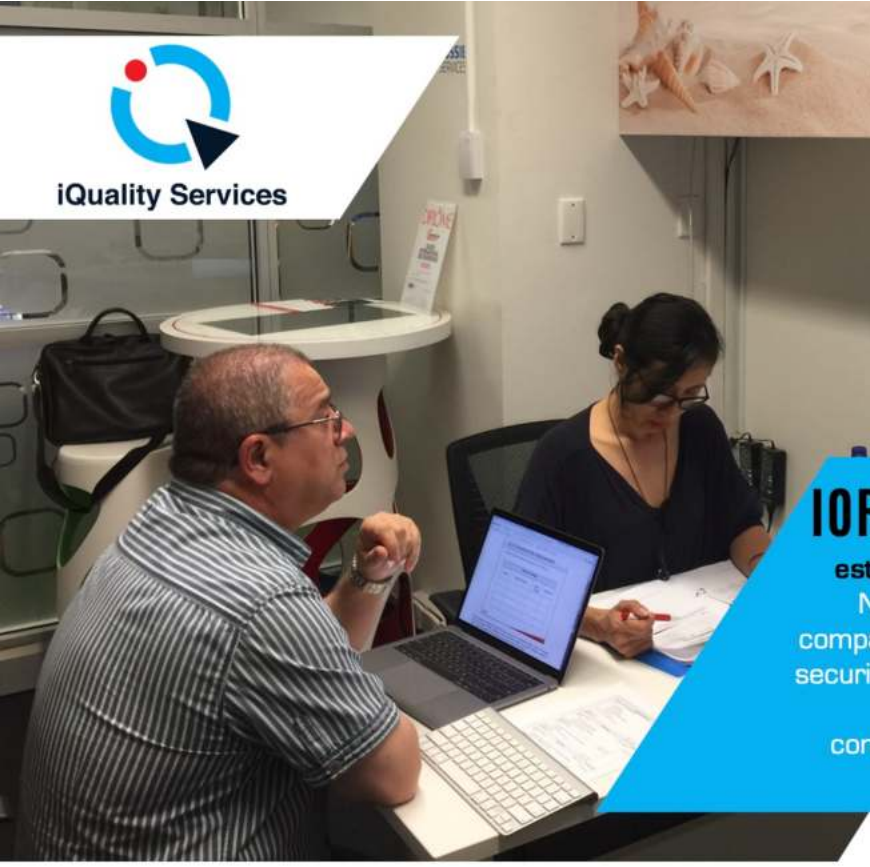
www.rqmcert.com

BIBLIOGRAFIE



- **SR ISO 31000:2018** Managementul riscului. Linii directoare.
- **SR EN IEC 31010:2020** Managementul riscului. Tehnici de evaluare a riscului.
- **SR Ghid ISO 73:2010** Managementul riscului. Vocabular.
- **Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Enterprise Risk Management**, by Clive Thompson and Paul Hopkin, 2021.
- **ISO 31000: 2018 Enterprise Risk Management (CERM Academy Series on Enterprise Risk Management),** by Greg Hutchins, 2018.
- **Enterprise Risk Management in Government: Implementing ISO 31000:2018**, by James Kline, 2019.
- **Suport de curs „Managementul riscului și tehnici de evaluare a riscului”**, RQM Cert, 2022

iQuality Services



IORDACHE QUALITY SERVICES

este o companie de consultanţă independentă. Noi nu suntem parteneri şi/sau afiliaţi cu nicio companie furnizoare de servicii de securitate (pază, securitate electronică sau mecano-fizică, securitate la incendiu) astfel încât constatările noastre, concluziile şi recomandările se bazează numai pe interesul clientului nostru.

CONSULTANȚĂ DE SECURITATE

ASIGURAȚI-VĂ SECURITATEA CU iQUALITY SERVICES

Un furt, un jaf, o tâlhărie sau un act terorist nu are loc în fiecare zi, dar poate avea loc oricând.

NOI ÎȚI OFERIM SOLUȚII COMPLETE DE SECURITATE!

SERVICIILE NOASTRE DE CONSULTANȚĂ

Managementul Operațiunilor de Securitate

consultanţă de implementare a cerinţelor standardului internaţional „ISO 18788:2015 Management system for private security operations" care oferă un cadru pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, întreţinerea şi îmbunătăţirea gestionării operaţiunilor de securitate privată.

Sisteme de Management

consultanţă pentru implementarea în vederea certificării standardelor ISO 9001 - Sisteme de management al calităţii; ISO/IEC 27001 - Sisteme de management al securităţii informaţiei; ISO 14001 - Sisteme de management de mediu; ISO 37001 - Sisteme de management anti-mită şi Regulamentul general privind protecţia datelor (RGPD).

Sisteme de Securitate Private

consultanţă în întocmirea dosarelor de licenţiere IGPR; analiza si evaluarea riscurilor de securitate; alegerea soluţiilor tehnice de securitate electronică şi/sau fizică; managementul proiectelor de securitate; elaborarea politicilor şi procedurilor de securitate; Crime Prevention Through Environmental Design (CPTED).

CONTACTAȚI-NE!

+40 752 631 096

www.ioniordache.com

ion@ioniordache.com

RQM CERT

Your Knowledge Provider

YOUR KNOWLEDGE PROVIDER

RQM Cert este un furnizor de formare profesională cu o echipă de specialiști cu experiență în servicii de pregătire profesională, evaluare și audit. Avem cunoștințe în sisteme de management al calității, mediu, sănătate și siguranță ocupațională, auto, securitate fizică, a informațiilor, protecției datelor și serviciilor IT.

Programele noastre de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice industriei.

Classroom Training

RQM Cert deliver high-quality worldwide classroom trainings at various locations.

Self-study Training

Self-studying is an excellent way to highlight personal drive and intellectual curiosity when applying to training courses.

In-House Training

RQM Cert provides woldwide in-house courses, delivered by our trainers directly at your facility.

Virtual Classroom

Our Virtual Classroom training is the perfect method for you to participate in highly valuable learning from anywhere in the world to enhance skills.

DOMENIILE NOASTRE DE FORMARE

- ❑ Security & Fire Protection
- ❑ Automotive
- ❑ Project Management
- ❑ Service Management
- ❑ Information Security
- ❑ Cybersecurity
- ❑ Continuity, resilience, and recovery
- ❑ Governance, risk, and compliance
- ❑ Privacy and Data Protection
- ❑ Quality and Service Management
- ❑ Health and Safety
- ❑ Sustainability
- ❑ Cloud Credential Council (CCC)

CONTACT: +40 356 173 020 www.rqmcert.com office@rqmcert.com

Autor:

Ion Iordache, Ec

Consultant de Securitate,
Data Protection Officer (DPO) și Training & Development Manager la RQM Cert,
CEO și fondator la
Iordache Quality Services (iQS),
companii care oferă servicii de consultanță și cursuri de formare în managementul securității, GDPR și sisteme de management bazate pe standardele internaționale ISO.

www.ioniordache.com

ion@ioniordache.com
ion.iordache@rqmcert.ro

DATA ȘI VERSIUNEA 01.12.2022, V.00

Copii ale celei mai recente versiuni ale acestui ghid pot fi descărcate de pe https://ioniordache.com și https://rqmcert.com.

Dacă aveți nevoie de informații suplimentare, asistență sau recomandări cu privire la conținutul acestui document, vă rog să mă contactați.

RQM Certification

RQM Certification cu sediul în Timișoara este un furnizor de formare profesională cu o echipă excepțională de specialiști cu mare experiență în formare profesională, servicii de evaluare și audit. Compania are expertiză în domeniul sistemelor de management al calității, al mediului, al sănătății și securității la locul de muncă, al automobilelor, al securității fizice, al informațiilor și al serviciilor IT. Programele de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice fiecărei industrii.

www.rqmcert.com

office@rqmcert.com

+40 356 173 020