

Document de Referință pentru ISO 31000

Titlul: Sistem de management al riscului conform ISO 31000

Introducere

Scop și domeniu de aplicare:

Standardul ISO 31000 oferă principii și linii directoare generale pentru managementul riscului. Acesta poate fi utilizat de orice organizație, indiferent de mărime, industrie sau sector, și se aplică tuturor tipurilor de riscuri. Scopul principal este de a ajuta organizațiile să își gestioneze riscurile în mod eficient pentru a proteja și a crea valoare pentru părțile interesate.

Definiții și termeni: Pentru claritate, acest document utilizează următorii termeni și definiții:

- **Risc:** Efectul incertitudinii asupra obiectivelor.
- **Managementul Riscului:** Activitățile coordonate pentru a direcționa și controla o organizație în ceea ce privește riscul.
- **Evaluarea Riscului:** Procesul general de identificare, analiză și evaluare a riscurilor.

Principii de management al riscului

- **Creați și protejați valoarea:** Managementul riscului ar trebui să contribuie la realizarea obiectivelor și la îmbunătățirea performanței generale a organizației, protejând și creând valoare pentru părțile interesate.
- **Integrați managementul riscului în procesele organizației:** Managementul riscului ar trebui să fie parte integrantă a tuturor proceselor organizaționale, de la planificare și gestionare până la raportare și îmbunătățire.
- **Abordați incertitudinea în mod sistematic și structurat:** Abordarea riscurilor trebuie să fie sistematică, structurată și bazată pe cele mai bune informații disponibile.

Cerințe generale

- **Imparțialitate și independență:** Organizația trebuie să asigure imparțialitatea și obiectivitatea în toate activitățile legate de managementul riscului. Politicile trebuie să fie stabilite pentru a preveni conflictele de interese și pentru a asigura că deciziile sunt luate fără influențe externe.
- **Confidențialitate:** Protejarea informațiilor sensibile și confidențiale este esențială. Organizația trebuie să aibă politici stricte pentru a preveni accesul neautorizat la date și pentru a asigura că toate informațiile sunt gestionate conform reglementărilor legale.

Cerințe structurale

- **Organizarea și responsabilitățile:** Organizația trebuie să aibă o structură organizatorică clar definită, cu roluri și responsabilități bine stabilite pentru managementul riscului. Organigrama trebuie să fie actualizată periodic pentru a reflecta schimbările și pentru a asigura eficiența operațiunilor.

- **Managementul riscurilor:** Identificarea și evaluarea riscurilor este crucială pentru prevenirea problemelor. Organizația trebuie să implementeze un sistem de management al riscurilor care include identificarea riscurilor potențiale, evaluarea impactului acestora și dezvoltarea de măsuri preventive și corective.

Cerințe de resurse

- **Personal:** Personalul implicat în managementul riscului trebuie să aibă calificările necesare și să participe la programe de formare continuă pentru a-și menține competențele. Fiecare angajat trebuie să fie evaluat periodic pentru a se asigura că îndeplinește standardele de performanță.
- **Infrastructură:** Organizația trebuie să dispună de resursele și infrastructura necesare pentru a susține managementul riscului. Aceasta include facilități adecvate, echipamente și tehnologie de suport.

Cerințe procesuale

- **Identificarea riscurilor:** Organizația trebuie să stabilească un proces continuu de identificare a riscurilor care ar putea afecta atingerea obiectivelor. Acest proces trebuie să implice toate părțile relevante și să utilizeze metode adecvate pentru colectarea și analiza datelor.
- **Evaluarea și analiza riscurilor:** Evaluarea riscurilor include analiza și clasificarea riscurilor identificate în funcție de probabilitatea și impactul lor. Aceasta ajută la prioritizarea riscurilor și la alocarea resurselor pentru gestionarea acestora.
- **Tratamentul riscurilor:** Organizația trebuie să dezvolte și să implementeze planuri de tratament pentru a aborda riscurile identificate. Aceste planuri pot include evitarea riscurilor, reducerea impactului acestora, transferul riscurilor sau acceptarea acestora.
- **Monitorizarea și revizuirea:** Monitorizarea continuă a riscurilor și a măsurilor de tratament este esențială pentru a asigura eficacitatea managementului riscului. Organizația trebuie să revizuiască periodic procesul de management al riscului pentru a identifica oportunități de îmbunătățire.

Managementul calității

- **Sistemul de management al calității:** Implementarea unui sistem de management al calității este esențială pentru conformitatea cu ISO 31000. Acesta trebuie să includă politici și proceduri pentru toate aspectele legate de managementul riscului, de la identificare până la monitorizare.
- **Controlul documentelor:** Documentele și înregistrările trebuie să fie gestionate riguros pentru a asigura că sunt corecte și disponibile atunci când este necesar. Organizația trebuie să aibă proceduri pentru crearea, revizuirea, aprobarea și distribuția documentelor.
- **Îmbunătățirea continuă:** Organizația trebuie să se angajeze în îmbunătățirea continuă a proceselor și metodologiilor utilizate pentru managementul riscului. Acest lucru poate include evaluări periodice, feedback-ul angajaților și al părților interesate, și implementarea de acțiuni corective și preventive.

Evaluare și Audit

- **Audit intern:** Auditurile interne sunt esențiale pentru a verifica conformitatea cu cerințele ISO 31000. Organizația trebuie să planifice și să efectueze audituri interne regulate pentru a evalua eficacitatea sistemului de management al riscului și pentru a identifica oportunități de îmbunătățire.
- **Revizuirea managementului:** Managementul organizației trebuie să revizuiască periodic performanța sistemului de management al riscului. Această revizuire trebuie să includă evaluarea rezultatelor auditului intern, feedback-ul părților interesate și identificarea acțiunilor necesare pentru îmbunătățire.

Managementul neconformităților

- **Identificarea și controlul neconformităților:** Procedurile pentru identificarea și controlul neconformităților trebuie să fie bine definite. Organizația trebuie să documenteze toate neconformitățile, să analizeze cauzele acestora și să implementeze acțiuni corective pentru a preveni recurența.
- **Acțiuni corective și preventive:** Organizația trebuie să dezvolte și să implementeze acțiuni corective și preventive bazate pe analiza cauzelor neconformităților. Aceste acțiuni trebuie să fie monitorizate și evaluate pentru a asigura eficacitatea lor.

Satisfacția părților interesate

- **Feedback-ul părților interesate:** Colectarea și analiza feedback-ului de la părțile interesate este crucială pentru îmbunătățirea managementului riscului. Organizația trebuie să aibă proceduri pentru a colecta feedback-ul și pentru a-l folosi în evaluarea performanței.
- **Îmbunătățirea satisfacției părților interesate:** Organizația trebuie să implementeze măsuri pentru a îmbunătăți satisfacția părților interesate. Acestea pot include îmbunătățiri în comunicare, transparența proceselor și asigurarea unei experiențe pozitive pentru toate părțile implicate.