

**METODE**



**MEHARI 2010**  
**PRIVIRE GENERALĂ**

Noiembrie 2010



Comision Metodelor

**CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS**

11, rue de Mogador, 75009 PARIS (France)

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : [clusif@clusif.asso.fr](mailto:clusif@clusif.asso.fr)

Web : <http://www.clusif.asso.fr>

Mehari este marcă înregistrată a CLUSIF**MULȚUMIRI**

Clusif ar dori să mulțumească în special lui Jean-Philippe Jouas pentru contribuția sa, lui Jean-Louis Roule pentru traducere cât și membrilor comisiei Metodelor care au participat la realizarea acestui document.

Traducerea în limba română a fost realizată de **Cînipariu Petronela** și **Grigoraș Anca-Laura**, studenți ai Facultății de Economie și Administrarea Afacerilor din cadrul Universității Alexandru Ioan Cuza din Iași.

Proiectul a fost coordonat de **drd. Alina Marin** și **dr. Valentin-Petru Măzăreanu**, cercetător postdoc și cadru didactic asociat în instituția mai sus menționată.

Contact:

[www.managementul-riscurilor.ro](http://www.managementul-riscurilor.ro)

[www.feaa.uaic.ro](http://www.feaa.uaic.ro)

[vali.mazareanu@feaa.uaic.ro](mailto:vali.mazareanu@feaa.uaic.ro)

## CUPRINS

<u>1.INTRODUCERE.....</u>	<u>4</u>
<u>2.UTILIZĂRI ALE MEHARI.....</u>	<u>5</u>
<u>2.1 Analiza sau evaluarea riscului.....</u>	<u>6</u>
<u>2.1.1 Analiza sistematică a situațiilor de risc.....</u>	<u>6</u>
<u>2.1.2 Analiza spontană a situațiilor de risc.....</u>	<u>7</u>
<u>2.1.3 Analiza riscului în proiecte noi.....</u>	<u>7</u>
<u>2.2 Evaluări ale securității.....</u>	<u>7</u>
<u>2.2.1 Recenzia vulnerabilității, un element de analiză a riscului.....</u>	<u>7</u>
<u>2.2.2 Planuri de securitate bazate pe recenzii ale vulnerabilității.....</u>	<u>7</u>
<u>2.2.3 Suport oferit de bazele de cunoștințe în crearea unor cadre de referință a securității.....</u>	<u>8</u>
<u>2.2.4 Domenii acoperite de modulul de evaluare a vulnerabilității.....</u>	<u>8</u>
<u>2.2.5 Privire de ansamblu asupra modulului de evaluare.....</u>	<u>8</u>
<u>2.3 Analizarea mizelor.....</u>	<u>9</u>
<u>2.3.1 Analizarea mizelor, baza pentru o analiză a riscului.....</u>	<u>10</u>
<u>2.3.2 Analiza mizelor de securitate: piatra de temelie pentru orice planificare de acțiune strategică.....</u>	<u>10</u>
<u>2.3.3 Clasificare: un element esențial pentru politica de securitate.....</u>	<u>10</u>
<u>2.3.4 Analiza mizelor de securitate: baza planificării securității.....</u>	<u>10</u>
<u>2.4. Prezentare generală a utilizărilor MEHARI.....</u>	<u>11</u>
<u>3.MEHARI și ISO/IEC 27000 STANDARDS.....</u>	<u>12</u>
<u>3.1 Obiectivele respective ale lui ISO / IEC 27001,27002,27005 și MEHARI.....</u>	<u>12</u>
<u>3.1.1 Obiectivele standardului ISO / IEC 27002:27005 .....</u>	<u>12</u>
<u>3.1.2 Scopuri ale ISO / IEC 27001:2005.....</u>	<u>12</u>
<u>3.1.3 Scopurile ISO / IEC 27005:2008.....</u>	<u>13</u>
<u>3.1.4 Scopurile MEHARI.....</u>	<u>13</u>
<u>3.1.5 Comparatie a obiectivelor MEHARI standardele ISO / IEC 27001 și 27002 .....</u>	<u>14</u>
<u>3.2. Compatibilitatea dintre aceste abordări.....</u>	<u>14</u>
<u>3.2.1 Compatibilitatea cu standardul ISO / IEC 27002:2005 .....</u>	<u>14</u>
<u>3.2.2 Compatibilitatea cu standardul ISO/IEC 27001.....</u>	<u>14</u>
<u>3.2.3 Compatibilitatea cu standardul ISO/IEC 27005:2008.....</u>	<u>15</u>

## 1.INTRODUCERE

Metodologia MEHARI a fost proiectată inițial și este actualizată în permanență pentru a asista Ofițerii-Şef de Securitate a Informațiilor (CISO), în gestionarea sarcinilor de securitate a informațiilor.

Acest rezumat este destinat în principal lor, dar este, de asemenea, destinat și auditorilor, CIO sau managerilor de risc care împărtășesc în mare parte aceleași provocări sau unele similare.

Principalul scop al acestui document este de a descrie modul în care MEHARI poate fi utilizat. O descriere mai detaliată a metodologiei și a uneltelor asociate este prevăzută în alte documente disponibile la Clusif, în special:

- MEHARI: Concepte și Specificații funcționale,
- MEHARI: Ghiduri pentru:
  - analiza mizelor și clasificare,
  - evaluarea serviciilor de securitate și
  - analiza riscului,
- MEHARI: Manual de referință al serviciilor de securitate,
- MEHARI cunoștințe de bază

Principalul obiectiv al MEHARI este de a furniza o evaluare a riscurilor și o metodă de gestionare, specifice domeniului securității informațiilor, conforme cu cerințele ISO/IEC 27005:2008 și oferind setul de unelte și elemente necesare pentru implementarea sa.

Obiectivele suplimentare sunt:

Să permită o analiză directă și individuală a situațiilor de risc descrise de scenarii,

Să ofere un set complet de instrumente special concepute pentru managementul securității pe termen scurt, mediu și lung, adaptabile la diferite niveluri de maturitate și tipuri de acțiuni considerate.

Intr-adevăr, MEHARI furnizează o metodologie consistentă, cu baze de date adecvate de cunoștințe, pentru a veni în ajutor Ofițerilor Șefi în Securitatea Informațională, directorilor generali și managerilor de securitate sau alte persoane implicate în reducerea riscurilor, în diferitele lor sarcini și acțiuni.

Raportul dintre MEHARI și standardele ISO/IEC 27000 este descris la sfârșitul documentului.

## 2.UTILIZĂRI ALE MEHARI

MEHARI este mai presus de toate o metodă de evaluare și management a riscului.

***In practică, aceasta înseamnă că MEHARI și bazele sale de cunoștințe asociate au fost concepute pentru o analiză precisă a situațiilor de risc descrise prin scenarii.***

În termeni de zi cu zi, managementul securității este o funcție sau activitate care evoluează de-a lungul timpului. Acțiunile corective sunt diferite în funcție de faptul dacă organizația a făcut ceva în domeniu sau – dimpotrivă – a făcut investiții substanțiale în ceea ce privește timpul și efortul. În parcurgerea primilor pași în securitate este fără îndoială recomandabil să se țină seama de starea măsurilor de securitate existente și politicilor organizației, și să se compare cu cele mai bune practici, pentru a clarifica golul care trebuie umplut.

În urma acestei evaluări a stării și a deciziei de a implementa securitatea organizațională, acțiuni concrete vor trebui să fie decise. Astfel de decizii, care vor fi grupate de obicei în planuri, reguli corporatiste, politici sau de un cadru de referință al securității, ar trebui să se facă cu ajutorul unei abordări structurate. Aceasta abordare se poate baza pe analiza riscului, așa cum este solicitat de ISO/IEC 27001 ca parte a ISMS (Sistemul de Management al Securității Informaționale). Există și alte mijloace, precum compararea, fie internă, profesională sau inter-profesională.

În acest stadiu, este adevărat că, fără a menționa în mod deosebit analiza riscului, trebuie adresată problema mizelor implicate. Destul de des, indiferent de modul în care a fost luată decizia, persoana căreia îi aparține decizia finală pentru alocarea bugetului corespunzător va pune fără îndoială întrebarea: "este acest lucru cu adevărat necesar?". Din cauza lipsei unei evaluări preliminare a - și a unui consimțământ general asupra - mizelor implicate, multe proiecte de securitate sunt abandonate sau amânate.

Deseori mai târziu, dar uneori chiar de la începutul unei abordări a securității, riscul real la care organizația sau întreprinderea este expusă este pus la îndoială. Acest lucru este adesea formulat în termeni similari cu aceștia: "Au fost identificate toate riscurile la care este expusă organizația, și există vreo asigurare cum că nivelurile acestora sunt acceptabile?" Această întrebare ar putea fi la fel de ușor adresată la un nivel corporativ, sau cu referire la un anumit proiect. Se impune o metodologie care să includă analiza riscului.

MEHARI este fondat pe principiul că uneltele necesare fiecărui stadiu de dezvoltare a securității trebuie să fie consecvente. Prin aceasta se înțelege că orice rezultate generate la un anumit stadiu trebuie să fie reutilizabile mai târziu de către alte unelte sau oriunde altundeva în organizație.

**Diferitele unelte și module ale setului de metodologie MEHARI, concepute pentru a însoți o analiză directă și individuală a riscului, pot fi folosite separat una de cealaltă la orice pas al dezvoltării securității, folosind diferite abordări ale managementului, și garantează o consecvență a deciziilor rezultate.**

Toate aceste unelte și module – descrise pe scurt mai sus – alcătuiesc o metodă consecventă de evaluare a riscului împreună cu uneltele ajutoare necesare și module pentru analiza mizelor și de control a calității măsurilor de securitate, etc.

## 2.1 Analiza sau evaluarea riscului

Analiza riscului este menționată în aproape orice publicație referitoare la securitate, ca fiind forța motrice pentru a exprima cerințele de securitate și acest lucru este precizat din nou de către standardele ISO/IEC. Cu toate acestea, cele mai multe eșuează în a discuta despre ce metode ar trebui să fie utilizate.

Pentru mai mult de 15 ani, MEHARI a furnizat o abordare structurată de evaluare a riscului, bazată pe câteva principii simple.

O situație de risc poate fi caracterizată de diverși factori:

- Factori structurali (sau organizaționali), care nu depind de măsurile de securitate, ci de activitatea de bază a organizației, de mediul său și de contextul acesteia.
- Factori de reducere a riscului care reprezintă o funcție directă a măsurilor de securitate implementate.

De fapt, analiza mizelor de securitate este necesară pentru a determina nivelul de maximă seriozitate a consecințelor unei situații de risc. Acesta este de regulă un factor structural, în timp ce evaluarea securității va fi utilizată pentru a aprecia factorii de reducere a riscului.

MEHARI permite evaluarea calitativă și cantitativă a acestor factori și ca urmare ajută la evaluarea nivelurilor de risc. În acest sens, MEHARI integrează instrumente (precum criteriile de evaluare, formule, etc) și baze de cunoștințe (în special pentru diagnosticarea măsurilor de securitate), care sunt completări esențiale pentru cadrul minim propus de ISO/IEC 27005.

### 2.1.1 Analiza sistematică a situațiilor de risc

În ideea de a răspunde la întrebarea "care sunt riscurile de deasupra organizației și sunt acestea acceptabile sau nu?", o abordare structurată este necesară pentru a identifica toate situațiile potențiale de risc, pentru a analiza în mod individual pe cele mai critice dintre acestea, și apoi pentru a identifica acțiuni de reducere a riscului la un nivel acceptabil.

Abordarea oferită de MEHARI se bazează pe o bază de cunoștințe cu situații de risc și pe proceduri automatizate pentru evaluare factorilor ce caracterizează fiecare risc și care permit aprecierea nivelului acestora. Mai mult decât atât, metoda oferă asistență pentru selecția planurilor de îngrijire adecvate.

Cu scopul de a evalua riscul, două opțiuni principale sunt propuse:

- Fie utilizați un set de funcții ale bazei de cunoștințe (pentru Microsoft Excel sau Open Office) care să permită să integreze rezultatele modulelor MEHARI (ex: clasificarea activelor din analiza mizelor, diagnostice de securitate). Pentru aceste funcții, este posibil să se evalueze nivelul actual de risc și să se propună măsuri adiționale pentru reducerea riscului.
- Fie o aplicație software (precum RISICARE) care oferă o interfață cu utilizatorul mai amplă și care permite simulări, vizualizări și optimizări ulterioare.

### 2.1.2 Analiza spontană a situațiilor de risc

Același set de instrumente poate fi folosit în orice moment în cadrul altor abordări de management a securității.

În unele moduri de pilotare a securității, unde managementul riscului nu este principalul obiectiv și unde securitatea este gestionată prin intermediul reviziilor sau cadrelor de referință a securității, vor exista adesea cazuri specifice unde regulile nu pot fi aplicate. Analiza spontană a riscului poate fi utilizată pentru a decide cum este cel mai bine să se procedeze.

### 2.1.3 Analiza riscului în proiecte noi

Modelul și mecanismele de analiză a riscului pot fi folosite în managementul proiectelor; pentru a planifica împotriva riscului și pentru a decide ce măsuri ar trebui utilizate ca urmare.

## 2.2 Evaluări ale securității

MEHARI integrează chestionare de diagnosticare amănunțită a controalelor de securitate, permițând evaluarea nivelului de calitate al mecanismelor și soluțiilor menite să reducă riscul.

### 2.2.1 Recenzia vulnerabilității, un element de analiză a riscului

MEHARI furnizează un model structurat de risc care ia în considerare "factorii de reducere a riscului", sub forma serviciilor de securitate.

Evaluarea rezultată a vulnerabilității va reprezenta, prin urmare, o contribuție importantă analiza riscului, asigurând faptul că serviciile de securitate își îndeplinesc într-adevăr rolul – un punct esențial pentru credibilitatea și fiabilitatea analizei riscului.

Un punct forte esențial al MEHARI este capacitatea sa de a evalua atât nivelul curent de risc, cât și nivelul viitor bazându-se pe o bază de cunoștințe expert fie de evaluare a nivelului de calitate, fie de operare sau decizie.

### 2.2.2 Planuri de securitate bazate pe recenzii ale vulnerabilității

O posibilă abordare este de a construi planuri de acțiune direct ca urmare a evaluării stării serviciilor de securitate.

Procesul de management a securității care urmează această abordare este extrem de simplu: rulează o evaluare și decide să îmbunătățească toate acele servicii care nu au un nivel de calitate suficient.

Chestionarele de diagnosticare MEHARI pot fi utilizate în această abordare.

O analiză preliminară a mijloacelor de afaceri ar trebui să fie planificată, de asemenea, pentru a oferi astfel o legătură către acest modul al MEHARI. Analiza mijloacelor permite constatarea nivelurilor de calitate necesare pentru serviciile de securitate relevante și, în consecință, ca ceilalți să fie ignorați în calitate de parte a evaluării.

### 2.2.3 Suport oferit de bazele de cunoștințe în crearea unor cadre de referință a securității

Baza de cunoștințe unică MEHARI poate fi utilizată în mod direct pentru a crea un cadru de referință al securității (sau politici de securitate) care să conțină și să descrie setul de reguli de securitate și instrucțiuni pe care întreprinderea sau organizația le va urmări.

Această abordare este adesea utilizată în organizații sau întreprinderi cu un număr de site-uri sau unități operaționale independente. Acesta ar fi, în mod tipic, cazul companiilor multinaționale mari cu un număr de filiale; dar se aplică la fel de ușor companiilor de dimensiuni medii cu un număr mare de sucursale sau agenții regionale. În astfel de cazuri, este efectiv dificil să se efectueze numeroase evaluări sau analize de risc.

#### **Construirea cadrului de referință al securității**

Chestionarele de evaluare MEHARI sunt o bună bază de lucru pentru managerii de securitate pentru a decide ce ar trebui să fie aplicat în organizația lor.

#### **Gestionarea excepțiilor de la reguli**

Crearea unui set de reguli, prin intermediul unui cadru de referință al securității, de multe ori vine împotriva dificultăților locale de implementare; așadar, derogările și excepțiile de la reguli trebuie gestionate.

Utilizarea unei baze de cunoștințe coerentă, cu un set consistent de instrumente și metodologie analitică, oferă posibilitatea ca divergențele locale să fie gestionate. Cererile pentru excepții pot fi incluse într-o analiză specifică a riscului, axată pe dificultatea identificată.

### 2.2.4 Domenii acoperite de modulul de evaluare a vulnerabilității

Dintr-un punct de vedere al analizei riscului, referitor la identificarea tuturor situațiilor de risc și dorinței de a acoperi toate riscurile inacceptabile, MEHARI nu se limitează pur și simplu la domeniul IT.

Modulul de evaluare include, în afară de sistemul de informații, organizația în ansamblu și protecția site-ului în general, precum și mediul de lucru și aspecte juridice și de reglementare.

### 2.2.5 Privire de ansamblu asupra modulului de evaluare

Singurul lucru ce trebuie avut în vedere cu privire la modulul de evaluare a securității este acela că oferă o perspectivă extinsă și consecventă asupra securității. Aceasta poate fi utilizată într-o varietate de abordări, evolutive în profunzimea și granularitatea analizei, și poate fi utilizată în toate stadiile de maturitate ale conștientizării și organizării securității întreprinderii.

## 2.3 Analizarea mizelor

Securitatea se refera la protejarea activelor. Indiferent de orientările politicii de securitate, există un principiu asupra căruia toți managerii sunt de acord; că trebuie să existe un echilibru doar între investițiile în securitate pe de o parte și importanța mizelor de afaceri relevante.

Aceasta înseamnă că o înțelegere corespunzătoare a mizelor de afaceri este fundamentală, și că o analiză a mizelor de securitate merită un nivel de prioritate înalt și o metodă strictă și structurată de evaluare.

Scopul analizei mizelor de securitate este de a răspunde la două întrebări:

### **"Ce s-ar putea întâmpla, și dacă a făcut-o, ar fi serios?"**

Acest lucru arată că, în domeniul securității, mizele sunt văzute ca fiind consecințele evenimentelor care deranjează operațiunile planificate ale unei întreprinderi sau organizații.

*MEHARI* oferă un modul de analiză a mizelor, descris în *MEHARI: Analiza mizelor și clasificare*, care produce două tipuri de rezultate:

- O scală a defecțiunilor
- O clasificare a informației și a bunurilor IT

### **Scala defecțiunilor**

Identificarea defecțiunilor sau a evenimentelor potențiale este un proces care începe cu activitățile întreprinderii și constă în identificarea posibilelor defecțiuni din procesele sale operaționale. Aceasta va duce la:

- O descriere a tipurilor de defecțiuni posibile
- O definiție a parametrilor care influențează gravitatea fiecărei defecțiuni
- O evaluare a pragurilor critice a acelor parametri care schimbă nivelul de gravitate al defecțiunii.

Acest set de rezultate constituie o scară de valori a defecțiunilor.

### **Clasificarea informației și a bunurilor**

Este de obicei, în sistemul IT de securitate, a vorbi de clasificarea informațiilor și de clasificarea bunurilor IT.

O astfel de clasificare constă în definirea, pentru fiecare tip de informații și pentru fiecare bun IT, și pentru fiecare criteriu de clasificare (clasic: Disponibilitate, Integritate, și Confidențialitate deși alte criterii pot fi utilizate, cum ar fi trasabilitatea), indicatorilor reprezentativi a criteriului gravității care este afectat sau pierdut pentru această informație sau activ.

Clasificarea informației și a bunurilor, pentru sistemele de informații, este scara de valori a defecțiunilor definită mai devreme tradusă în indicatori de sensibilitate asociați cu bunurile IT.

## **Exprimarea mizelor de securitate**

Scara de valori a defecțiunilor și clasificarea informației și a bunurilor sunt două moduri distincte de exprimare a mizelor de securitate.

Prima este mai detaliată și oferă mai multe informații pentru CISOs. Acesta din urmă este mai globală și mai utilă pentru campanii de sensibilizare și de comunicare, dar este mai puțin granuloasă.

### **2.3.1 Analizarea mizelor, baza pentru o analiză a riscului**

În mod clar, acest modul este un element cheie în analiza riscului. Fără un acord comun asupra consecințelor defecțiunilor potențiale, nici o hotărâre privind nivelurile de risc Vagonul posibil.

MEHARI prezintă o metodă riguroasă de evaluare a mizelor și clasificare a activelor, care oferă rezultate obiective și raționale.

### **2.3.2 Analiza mizelor de securitate: piatra de temelie pentru orice planificare de acțiune strategică**

Evident, analizarea mizelor este necesară pentru punerea în aplicare orice formă de plan de securitate.

Efectiv, orice abordare este folosită, la un moment dat, înseamnă ca va trebui să fie alocate pentru punerea în aplicare a planurilor de acțiune, și inevitabil, justificarea pentru astfel de investiții va fi pusă la îndoială.

Mijloacele și fondurile care vor fi alocate pentru securitate sunt, ca și pentru polițele de asigurare, în direct proporțional cu riscul. În cazul în care nu există un acord comun asupra potențialului defecțiunilor, atunci este foarte puțin probabil ca bugetele vor fi alocate.

### **2.3.3 Clasificare: un element esențial pentru politica de securitate**

Cadrele de referință de securitate, politicile de securitate, și abordarea asociate managementul securității au fost deja menționate în acest document.

În practică, companiile care administrează securitatea printr-un set de reguli sunt obligate să diferențieze, în ele însele normele, între acțiunile care urmează să fie efectuate ca o funcție de sensibilitate al informațiilor prelucrate. Este obișnuit să se facă referire la o clasificare a informațiilor și activelor sistemului IT.

Modulul MEHARI al analizei mizelor de securitate oferă mijloacele pentru a efectua această clasificare.

### **2.3.4 Analiza mizelor de securitate: baza planificării securității**

Proces de analiză a mizelor de securitate, care necesită în mod evident contribuția managerilor operaționali, de foarte multe ori duce la nevoia de acțiune imediată.

Experiența arată că, atunci când managementul operațional de top au fost intervievate, indiferent de mărimea organizației, și-au explicat punctul de vedere și estimarea de defecțiuni grave, acest lucru conduce la nevoi de securitate pe care aceștia nu au considerat anterior și care necesită răspunsuri rapide.

Planurile de acțiune pot fi apoi create direct, folosind o abordare ușoară și directă bazată pe combinarea a două seturi de expertiză: aceea a profesiei înseși, oferită de managementul operațional, și de soluții de securitate, oferite de experții în securitate.

## 2.4. Prezentare generală a utilizărilor MEHARI

În mod clar, principala orientare MEHARI este evaluarea riscurilor și de reducere. Bazele sale de cunoștințe, mecanismele și uneltele au fost create în acest scop.

De asemenea, în miștile designerilor setului de metodologii, necesitatea pentru o metodă structurată pentru analiza și reducerea riscului poate fi, în funcție de organizație:

- O metodă de lucru permanent-liniile directoare pentru un grup specializat,
- O metodă de lucru folosită în paralel cu alte practici de management al securității,
- O metodă de lucru folosită ocazional pentru a completa practicile obișnuite.

Având în vedere acest lucru, MEHARI oferă un set de abordări și instrumente de analiză a riscului care să permită să se facă atunci când este nevoie.

Metodologia MEHARI, cuprinzând bazele de cunoștințe, manualele și ghidurile care descriu diferitele module (mize, riscuri, vulnerabilități), este aici pentru a ajuta persoanele implicate în managementul securității (CISO, manageri de risc, auditori, CIO ,...) , în diferitele lor sarcini și acțiuni.

## 3.MEHARI și ISO/IEC 27000 STANDARDS

O întrebare care deseori este pusă: cum corespunde MEHARI standardelor internaționale, în special seriei ISO / IEC 27000.

Scopul aici este de a explica modul în care MEHARI se potrivește cu standardele ISO 27001,27002 și 27005, în termeni de compatibilitate și obiective.

### 3.1 Obiectivele respective ale lui ISO / IEC 27001,27002,27005 și MEHARI

#### 3.1.1 Obiectivele standardului ISO / IEC 27002:27005

Acest standard prevede că o organizație ar trebui să identifice cerințele de securitate folosind trei surse principale:

- Analiza de risc,
- Legale, statutare, de reglementare, sau cerințe contractuale,
- Set de principii, scopuri, și cerințe ce se aplică la procesarea informațiilor pe care organizația le-a dezvoltat pentru a sprijini operațiunile sale.

Folosind acest drept bază, punctele de control pot fi alese și implementate folosind lista prevăzută în secțiunea "cod de practică pentru managementul securității informaționale" din standard sau din orice alt set de puncte de control .

*NB: în domeniul de aplicare al 27002:2005, se stipulează că standardul oferă "liniile directoare și principiile generale pentru inițierea, implementarea, menținerea și îmbunătățirea managementului securității informaționale", ceea ce înseamnă că standardul ISO poate fi văzut ca un punct de plecare.*

*Cu toate acestea, ISO / IEC 27001 stipulează că orice excludere trebuie să fie justificată și că este acceptabil să se adauge puncte de control (Anexa A - A.1).*

Standardul ISO 27002 oferă o compilație de indicații, pe care o organizație le poate folosi. Acesta constată, totuși, că lista nu este exhaustivă, și că măsurile complementare pot fi necesare. Cu toate acestea, nici o metodologie nu este recomandată pentru crearea unui sistem complet de management de securitate.

Pe de altă parte, fiecare parte a ghidului de bune practici include introducere și comentarii cu privire la obiectivele propuse, care poate fi un ajutor foarte util.

*NB: Standardul ISO, de asemenea, prevede, în domeniul său de aplicare care poate fi folosit pentru a "ajuta la construirea încrederii în activități inter-organizaționale". Acest lucru nu este inclus din întâmplare, și scoate în evidență un aspect esențial că suporterii ai promoviei standard, care este evaluarea (chiar certificarea), din punct de vedere al securității informațiilor, de partenerii și furnizorii.*

#### 3.1.2 Scopuri ale ISO / IEC 27001:2005

Scopul clar al ISO / IEC 27001 este acela de a "oferi un model pentru a crea și administra un **sistem de management al securității informațiilor** ale companiei (**ISMS**)" și să fie "folosit fie intern sau de către terțe părți, inclusiv autoritățile de certificare".

Scopul de evaluare și certificare pune un puternic accent pe aspectele formale (documentația și înregistrarea deciziilor, declararea aplicabilității, registre, etc) și control (revizii, audituri, etc)

Este clar că baza abordării de securitate implică faptul că o analiză de risc trebuie să se desfășoare, pentru a examina riscurile la care organizația ar putea fi expusă, și pentru a selecta măsurile corespunzătoare pentru a reduce riscurile la un nivel acceptabil (paragraful 4.2.1) .

ISO / IEC 27001 stipulează că o metodă de analiză a riscului ar trebui să fie folosită, dar aceasta nu este o parte din standard, și nu este propusa nici o metodă specifică, în afară de integrarea PDCA (Planifica, Fa, Verifica, Actioneaza) proces recursiv a modelului astfel cum este definit pentru crearea ISMS.

De asemenea, recomandările sau cele mai bune practici care pot fi utilizate pentru a reduce riscul sunt "aliniate la cele enumerate în ISO / IEC 27002:2005", în timp ce o listă asociată cu punctele de control este prevăzută în anexe.

În conformitate cu ISO / IEC 27001, baza de **evaluare a sistemului de management al securității** nu este atât de mult cunoașterea sau verificarea faptului dacă deciziile care au fost efectuate sunt corespunzătoare și adaptate la nevoile organizației, ci mai degrabă pentru a verifica că, odată ce deciziile au fost realizate, sistemul de management este de așa natură încât un auditor sau certificator poate fi sigur că deciziile au fost implementate cu adevărat.

### 3.1.3 Scopurile ISO / IEC 27005:2008

Obiectivele acestui standard nu trebuie să constituie o metodă de gestionare a riscurilor ci, mai degrabă, să se stabilească un cadru minim și pentru a descrie cerințele, pentru procesul de evaluare a riscului în sine, pentru identificarea amenințărilor și vulnerabilităților care să permită estimarea riscurilor, nivelul lor și apoi să fie în poziția de a selecta un mod de tratament asociat și măsurători care vizează evaluarea și îmbunătățirea situației.

Standardul prevede că o metodă de evaluare a riscului trebuie să fie selectată în conformitate cu aceste cerințe în scopul de a evita utilizarea metodelor inconsistente sau simpliste, în comparație cu intenția editorilor standardului.

### 3.1.4 Scopurile MEHARI

MEHARI este un set consistent de instrumente și caracteristici metodologice pentru managementul securității și măsurilor asociate, pe baza unei analize de risc exacte. Aspecte fundamentale MEHARI:

- modelul său de risc (calitativ și cantitativ),
- luarea în considerare a eficienței măsurilor de securitate în loc sau planificate,
- capacitatea de a evalua și simula nivelurile de risc rezidual care rezultă din măsuri suplimentare,

sunt completari obligatorii la cerințele ISO / IEC 27000 și, în special de standarde ISO / IEC 27005.

### 3.1.5 Comparație a obiectivelor MEHARI standardele ISO / IEC 27001 și 27002

Scopurile MEHARI și ale standardelor ISO menționate mai sus sunt radical diferite.

- MEHARI țintește să ofere unelte și metode care pot fi folosite pentru a alege cele mai potrivite măsuri de securitate pentru o organizație dată și pentru a evalua riscurile reziduale odată ce aceste măsuri vor fi de operate. Acesta nu este obiectivul principal declarat al standardelor ISO.
- Standardele ISO oferă un set de bune practici, care sunt cu siguranță foarte utile, dar nu neapărat potrivite pentru ceea ce este în joc în organizație, sunt utile pentru a acoperi aspectele de maturitate în siguranță, planificarea informațiilor de securitate, unități independente interne și parteneri .

**Manualul de referință privind serviciile de securitate** MEHARI oferă eficiente elemente detaliate care pot fi folosite pentru a construi un cadru de securitate și poate fi comparat cu ISO / IEC 27002. La acest punct, este clar că acoperirea MEHARI este mai largă decât cea a ISO, și acoperă aspecte esențiale ale securității nu doar a sistemelor informaționale.

## 3.2. Compatibilitatea dintre aceste abordări

Abordarea MEHARI este complet compatibil cu ISO 27002 deoarece, în timp ce ei nu au aceleași obiective declarate, este relativ ușor să se reprezinte rezultatele unei analize MEHARI în ceea ce privește indicatorii ISO 27002.

MEHARI răspunde la necesitatea, exprimată în ambele standarde ISO 27001 și 27002, pentru o analiză a riscului pentru a defini măsurile care ar trebui să fie puse în aplicare.

### 3.2.1 Compatibilitatea cu standardul ISO / IEC 27002:2005

Punctele de control standard sau cele mai bune practici ale ISO sunt în general comportamentale sau organizaționale, în timp ce MEHARI, în plus față de ei, subliniază necesitatea unor măsuri a căror eficiență poate fi garantată.

În ciuda acestor diferențe, revizuirea vulnerabilității MEHARI oferă tabele de corespondență pentru a afișa indicatorii aliniați cu ISO 27002:2005, utilizabile pentru cei care au nevoie de a dovedi conformitatea lor cu acest standard.

Merită menționat aici despre chestionarele Mehari de audit care au fost concepute și constituite astfel încât să permită managerilor operaționali să ruleze revizuirile ale vulnerabilității și să deducă capacitatea fiecărui serviciu de securitate pentru a reduce aceste riscuri.

### 3.2.2 Compatibilitatea cu standardul ISO/IEC 27001

MEHARI poate fi integrat cu ușurință în procesele PDCA (Planifică – Execută – Verifică – Acționează) după cum se menționează în standardele ISO/IEC 27001, în special faza "PLANIFICĂ" (§4.2.1). Mehari acoperă în totalitate descrierea sarcinilor care permit crearea bazelor ISMS.

Pentru faza "EXECUTĂ" (§4.2.2) , care urmărește să implementeze și să administreze ISMS-ul, Mehari oferă elemente de început folositoare, precum construirea planurilor pentru managementul riscului, cu prioritizare direct legată de clasificarea riscului și măsurarea progresului în timpul de utilizare al acestora.

Pentru faza "VERIFICA" (§4.2.3) , Mehari oferă elemente care permit evaluarea riscurilor reziduale și a progreselor realizate în măsurile de securitate. În plus, orice schimbări ale mediului (mizele, amenințările, soluțiile și organizarea) pot fi reevaluate cu ușurință de auditurile vizate care folosesc rezultatele auditului Mehari inițial. Astfel, planurile de securitate pot fi revizuite și pot evolua în timp.

Pentru faza "ACȚIONEAZĂ" (§4.2.4), Mehari necesită implicit controale și îmbunătățire continuă a securității, asigurând astfel că obiectivele de reducere a riscurilor sunt îndeplinite. În aceste trei faze, cât timp Mehari nu se află în centrul proceselor, are o mare contribuție la execuția lor și le asigură eficiența.

### **3.2.3 Compatibilitatea cu standardul ISO/IEC 27005:2008**

Cadrul stabilit de acest nou standard este pe deplin aplicabil modului în care Mehari permite gestionarea riscului, de exemplu:

- Procesele pentru analiza, evaluarea și tratamentul riscului (preluate din ISO 13335)
- Identificarea activelor primare și de sprijin plus nivelurile de clasificare atașate acestora, urmărind analiza mizelor
- Identificarea amenințărilor incluzând nivelul lor (expunere naturală) pentru care Mehari este mai precis în descrierea scenariilor de risc.
- Identificarea și cuantificarea eficienței măsurilor (sau controalelor) de securitate în reducerea vulnerabilităților
- Combinația acestor elemente pentru evaluarea nivelului de gravitate a scenariilor de risc, pe o scară cu 4 niveluri.
- Abilitatea de a selecta în mod direct măsurile de securitate necesare pentru planurile de reducere a riscului.

Prin urmare, MEHARI nu este doar integrat cu ușurință într-un proces ISMS, așa cum e promovat de ISO 27001, ci se și conformă în totalitate cu cerințele ISO 27005 în legătură cu o metodă de management a riscului.



L'ESPRIT DE L'ÉCHANGE

## **CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS**

11, rue de Mogador  
75009 Paris France  
☎ + 33 1 53 25 08 80  
clusif@clusif.asso.fr

[www.clusif.asso.fr](http://www.clusif.asso.fr)