



# MEHARI 2007

## Privire Generală

**Recunoaştere**

CLUSIF doreşte să mulţumească membrilor echipei de lucru care au contribuit la crearea acestui document.

CLUSIF doreşte de asemenea să mulţumească dlui. Valentin P. Măzăreanu şi echipei sale (Alina Marin, Raluca Ungureanu) care au acceptat să furnizeze această traducere. Dl. Valentin P. Măzăreanu îşi desfăşoară activitatea în cadrul Facultăţii de Economie şi Administrarea Afacerilor, Universitatea „Al.I.Cuza" Iaşi şi este director general al Paideia Consulting Iaşi. Pentru mai multe informaţii despre activitatea dlui. Valentin P. Măzăreanu vă invităm să accesaţi www.managementul-riscurilor.ro.

Vă rugăm să trimiteţi întrebările şi comentariile dumneavoastră la adresa mehari@clusif.asso.fr

# Cuprins

# 1 Introducere

MEHARI a fost conceput inițial pentru a ajuta Ofițerii Șefi în Securitate Informațională (CISO) la sarcinile lor de management al securității sistemului informațional. El se află într-o evoluție continuă, pentru a satisface natura evolutivă a mediului de afaceri.

Acest rezumat este destinat în principal pentru CISO, dar el este şi pentru auditorii sau managerii de risc care se confruntă în mare cu aceleaşi provocări sau cu unele asemănătoare.

Principalul scop al acestui document este de a descrie pe scurt modul în care MEHARI poate fi folosit. O descriere mai detaliată a metodologiei şi a uneltelor asociate este oferită în alte documente disponibile de la Clusif, în special:

- *MEHARI; Concepte şi Mecanisme*
- *MEHARI: Analiza mizelor şi Ghidul de clasificare*
- *MEHARI: Ghidul de evaluare pentru serviciile de securitate*
- *MEHARI: Ghidul Analizei Riscului*
- *MEHARI: Baze de cunoştinţe şi Manuale cu referinţe (servicii de securitate şi scenarii de risc).*

MEHARI doreşte să ofere un set de unelte concepute specific pentru managementul securității, care cuprinde un set de acțiuni manageriale, fiecare cu un scop specific.

Câteva exemple pentru acestea sunt:

- Dezvoltarea planurilor de securitate, sau a planurilor strategice,
- Implementarea politicilor sau a regulilor de securitate, care vor fi grupate împreună sub termenul de „cadru de referință pentru securitate”,
- Desfăşurarea evaluărilor uşoare sau detaliate a stării securității,
- Evaluarea şi managementul riscului,
- Asigurarea includerii securității în managementul proiectelor aflate în dezvoltare,
- Conştientizarea securității şi sesiuni de training,
- Managementul operațional al securității şi controlul/monitorizarea acțiunilor săvârşite.

Aceste acțiuni manageriale, şi altele asemănătoare pot fi efectuate fie în paralel sau în serie, de grupuri specifice sau de acelaşi grup, în funcție de cerințele permanente sau specifice. În aceeaşi măsură, aceste acțiuni pot fi efectuate fie independent sau ca parte constituentă a unui program general.

Aceleaşi acțiuni manageriale pot fi efectuate în moduri diferite, în funcție de numărul de factori:

- Maturitatea, în ceea ce priveşte securitatea, a organizației şi a personalului său,
- Nivelul de implicare a conducerii în luarea deciziilor în securitatea informațională,
- Cultura întreprinderii: ierarhică şi tehnocrată (regulile există şi sunt aplicate), sau, dimpotrivă, descentralizată şi permisivă.

Dat fiind aceste diferențe, principala cerință a unei metodologii este de a veni cu un set însoțitor de unelte, potrivite pentru fiecare situație, consecvente şi complementare între ele, permițând mişcarea de la una la alta fără duplicarea sarcinilor sau muncă suplimentară.

MEHARI oferă o metodologie consecventă, cu baze de cunoştințe corespunzătoare, pentru a ajuta Ofițerii Șefi în Securitate Informațională (CISO), managerii generali, şi managerii de securitate, sau alte persoane implicate în reducerea riscului, la diferitele lor sarcini şi acțiuni.

Acest document oferă un rezumat al modului în care MEHARI poate fi folosit. Standardele internaționale aplicabile, şi relația MEHARI cu ele, sunt descrise pe scurt la sfârşitul documentului.

# 2 Utlizări ale Mehari

MEHARI este mai presus de toate o metodă pentru analiza riscului şi pentru managementul riscului.

**În practică, acest lucru înseamnă că MEHARI şi bazele sale de cunoştinţe asociate au fost menite pentru analiza exactă a riscului, atunci când este necesar, deşi fără a impune analiza riscului ca o prioritate a politicii de management.**

În termeni de zi cu zi, managementul securităţii este o funcţie sau activitate care evoluează în timp. Acţiunile manageriale sunt diferite în funcţie de faptul dacă organizaţia a făcut ceva în domeniu, sau – dimpotrivă – a făcut investiţii substanţiale în ceea ce priveşte timpul şi efortul.

Atunci când se fac primii paşi în securitate, este fără îndoială recomandabil să se evalueze starea măsurilor şi politicilor de securitate existente ale organizaţiei, şi să se compare cu cele mai bune practici, pentru a clarifica golul care trebuie umplut.

După această evaluare a stării şi decizia de a implementa securitatea organizaţională, se vor decide acţiunile concrete. Astfel de decizii, care vor fi grupate de obicei în planuri, reguli ale corporaţiei, politici sau un cadru de referinţă al securităţii, ar trebui luate folosind o abordare structurată. Această abordare se poate baza pe analiza riscului, sau poate include conceptul de risc, deşi nu este obligatoriu. Există şi alte mijloace, precum compararea, fie internă, profesională sau inter-profesională.

În acest stadiu, este adevărat că, fără a menţiona 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 aparţine decizia finală pentru alocarea bugetului corespunzător va pune fără îndoială întrebarea „este acest lucru cu adevărat necesar?”. Datorită lipsei unei evaluări preliminare a – şi a unui consimţământ general asupra – mizelor implicate, multe proiecte de securitate sunt abandonate sau amânate.

Deseori mai târziu, dar uneori chiar de la începutului unei abordări de securitate, riscul real pe care organizaţia sau întreprinderea şi-l asumă este pus sub semnul îndoielii. Acest lucru este deseori formulat în termeni asemănători cu următoarea frază: „Au fost identificate toate riscurile la care organizaţia ar putea fi expusă, şi există o oarecare asigurare că nivelurile acestora sunt acceptabile?”. Această întrebare ar putea la fel de uşor să fie adresată la nivelul corporaţiei, sau în legătură cu un anumit proiect. Este necesară o metodologie care include analiza riscului.

MEHARI este fundamentat pe principiul că uneltele necesare la fiecare stadiu de dezvoltare a securităţii trebuie să fie consecvente. Prin asta, se poate înţelege că orice rezultate generate la un anumit stadiu trebuie să fie reutilizabile de alte unelte mai târziu sau în altă parte în organizaţie.

**Diferitele unelte şi module a setului de metodologie MEHARI, concepute pentru a însoţi analiza riscului, pot fi folosite separat una de cealaltă la orice pas al dezvoltării securităţii, folosind diferite abordări de management, şi pot garanta o consecvenţă a deciziilor care rezultă.**

Toate aceste unelte şi module – descrise pe scurt mai jos – cuprind unelte pentru evaluarea stării securităţii, un modul pentru analizarea mizelor, şi o metodă de analiză a riscului cu uneltele ajutătoare.

## *2.1 Evaluările de securitate*

În setul MEHARI există două module de evaluare:

- Un modul de evaluare rapidă[1]
- Un modul de evaluare mai detaliată

În fiecare din cazuri, scopul este evaluarea nivelului securității. În practică, evaluarea va analiza serviciile de securitate. În mod clar, rezultatele vor depinde de profunzimea evaluării: dacă este mai rapidă, este mai puțin precisă; dacă este detaliată, este mai de încredere.

Primul modul ar trebui folosit pentru o evaluare rapidă a principalelor slăbiciuni, sau „o recenzie a vulnerabilităților". Serviciile de securitate care sunt examinate sunt aceleaşi cu cele pentru evaluarea detaliată, sau audit, dar întrebările au scopul de a afla dacă funcția de securitate a fost implementată fără a fi validată pentru slăbiciuni. În acest sens, orice slăbiciuni identificate sunt cu siguranță slăbiciuni, dar punctele tari potențiale pot să nu fie puncte tari.

Modulul evaluării detaliate caută, în detaliu, posibilele slăbiciuni ale fiecărui serviciu de securitate individual. El constituie astfel o bază de expertiză, utilizabilă pentru analiza riscului.
Consecvența dintre aceste două module permite ca prima abordare să fie folosită ca un punct de plecare, şi apoi să repete în profunzime în orice moment, şi pentru orice punct care poate necesita asigurare.
Modulele de evaluare pot fi folosite în mai multe moduri[2].

### 2.1.1 Recenzia vulnerabilității, un element al analizei riscului

MEHARI oferă o metodă de analiză a riscului structurată care va fi explicată mai târziu. În acest moment, ar trebui să fie suficient a se şti faptul că modelul riscului ia în considerare "factori de reducere a riscului", sub forma serviciilor de securitate.

Evaluarea detaliată va fi deci un adaos important pentru analiza riscului la asigurarea faptului că serviciile de securitate îşi îndeplinesc cu adevărat rolul – un punct esențial pentru credibilitatea analizei riscului.

### 2.1.2 Planuri de securitate pe baza trecerilor în revistă ale vulnerabilităților

O abordare relativ populară este de a construi planuri de acțiune direct ca rezultat al evaluării stării serviciilor de securitate.

Procesul de management al securității care urmează această abordare este extrem de simplu: efectuează o evaluare şi decide să îmbunătățeşti toate acele servicii care nu au un nivel al calității suficient de bun.

Utilizarea analizei preliminare a mizelor de securitate este şi ea planificată, oferind astfel o legătură cu acest modul al MEHARI (descrisă mai târziu în acest document).

Stadiile diferite şi sfaturile pentru implementarea acestei forme de management sunt descrise în *MEHARI – Ghidul de Evaluare pentru serviciile de securitate.*

[1] Acest modul se află momentan în dezvoltare
[2] Trecerile în revistă ale vulnerabilității sunt descrise în MEHARI – Ghidul de evaluare pentru serviciile de securitate

### 2.1.3 Sprijin oferit de bazele de cunoştinţe în crearea unui cadru de referinţă pentru securitate

Modulul de evaluare detaliată utilizează baza de cunoştinţe a serviciilor de securitate (documentată în *MEHARI – manualul de referinţe pentru servicii de securitate*[3]). Acesta descrie, pentru fiecare serviciu, la ce foloseşte, împotriva a ce este folosit, mecanismele şi soluţiile care sprijină serviciul, şi acele elemente care ar trebui considerate atunci când se evaluează calitatea serviciului.

Această bază de cunoştinţe unică poate fi folosită direct pentru a crea un cadru de referinţă pentru securitate (sau politici de securitate) care va conţine, şi va descrie, setul de reguli şi instrucţiuni de securitate pe care întreprinderea sau organizaţia le va urma.

Această abordare este deseori folosită în organizaţii sau întreprinderi cu mai multe unităţi sau site-uri operaţionale independente. Acesta ar fi de obicei cazul pentru companiile multinaţionale mari cu mai mulţi afiliaţi; dar se aplică la fel de uşor pentru companiile medii cu un număr mare de filiale sau agenţii regionale. În astfel de cazuri, este greu să se efectueze numeroase evaluări sau analize ale riscului.

***Construirea cadrului de referinţă al securităţii***

Chestionarele de evaluare şi, mai presus de toate, manualul de referinţe pentru servicii de securitate cu explicaţiile suplimentare pe care le oferă reprezintă o bună bază de lucru pentru managerii de securitate pentru a decide ce ar trebui aplicat în organizaţia lor.

***Administrarea excepţiilor de la regulă***

Crearea unui set de reguli, printr-un cadru de referinţă pentru securitate, intră deseori în conflict cu dificultăţile de implementare locale; aşa că, trebuiesc administrate abandonuri şi excepţii de la reguli.

Utilizarea unei baze de cunoştinţe coerente, cu un set de unelte consecvent şi o metodologie analitică, permite administrarea divergenţelor locale. Cererile pentru excepţii pot fi acoperite printr-o analiză a riscului specifică concentrată pe dificultatea identificată.

### 2.1.4 Domenii acoperite de modulul de evaluare

Din punctul de vedere al analizei riscului, în ceea ce priveşte toate situaţiile de risc şi dorinţa de a acoperi toate riscurile inacceptabile, MEHARI nu este restricţionat doar la domeniul IT.

Modulul de evaluare acoperă, în afară de sistemul informaţional, organizaţia în ansamblu, şi protecţia site-ului în general, precum şi mediul de lucru şi aspectele legale şi reglementatoare.

### 2.1.5 Rezumat al modulului de evaluare

Lucrul care trebuie reţinut în legătură cu modulul de evaluare este că oferă o privire largă şi consecventă asupra securităţii. Acest lucru poate fi folosit în mai multe abordări, care evoluează în ceea ce priveşte profunzimea şi granulozitatea analizei, şi poate fi folosit în toate stadiile de maturitate ale conştientizării securităţii întreprinderii şi a organizaţiei.

## *2.2 Analizarea mizelor*

Securitatea se referă la protecţia bunurilor. Oricare ar fi orientările politicii de securitate, există un

[3] Manualul de referinţe pentru serviciile de securitate face parte din bazele de cunoştinţe Mehari.

principiu asupra căruia toți managerii sunt de acord; acela că trebuie să existe un echilibru just între investițiile în securitate pe de o parte şi importanța mizelor de securitate în sine.

Acest lucru înseamnă că o înțelegere corespunzătoare a mizelor de securitate este fundamentală, şi că analiza mizelor de securitate merită un nivel ridicat al priorității şi o metodă de evaluare strictă şi structurată.

Scopul unei analize a mizelor de securitate este acela de a răspunde la dubla întrebare:

***„Ce s-ar putea întâmpla, şi dacă s-ar întâmpla, ar fi grav?".***

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 şi clasificare*, care produce două tipuri de rezultate:

- scară de valori a defecțiunilor
- clasificare a informației şi a bunurilor IT

***Scara de valori a defecțiunilor***

Identificarea defecțiunilor sau a evenimentelor potențiale este un proces care începe cu activitățile întreprinderii şi constă în identificarea posibilelor defecțiuni din procesele sale operaționale. Va rezulta în:

- descriere a tipurilor de defecțiuni posibile
- definiție a parametrilor care influențează gravitatea fiecărei defecțiuni
- 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 şi a bunurilor***

Este ceva obişnuit, în securitatea sistemului IT, să se vorbească despre clasificarea informației şi despre clasificarea bunurilor IT.

O astfel de clasificare constă în definirea, pentru fiecare tip de informație şi pentru fiecare bun IT, şi pentru fiecare criteriu de clasificare (în mod clasic: Disponibilitate, Integritate, şi Confidențialitate), a indicatorilor reprezentativi a gravității criteriului care este afectat sau pierdut pentru această informație sau bun.

Clasificarea informației şi a bunurilor, pentru sistemele informaționale, reprezintă 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 şi clasificarea informației şi a bunurilor reprezintă două moduri distincte de a exprima mizele de securitate.

Prima este mai detaliată şi oferă mai multe informații pentru CISO. Cea din urmă este mai globală şi mai utilă pentru campaniile de conştientizare şi comunicare, dar este mai puțin granuloasă.

## 2.2.1 Analizarea mizelor, baza pentru o analiză a riscului

În mod clar, acest modul este foarte important în analiza riscului. Fără un acord comun asupra

consecințelor defecțiunilor potențiale, nu va fi posibilă nici o judecată referitor nivelurile de risc.

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

După cum a fost descris în introducere, analizarea mizelor este foarte des necesară pentru implementarea oricărei forme a planului de securitate. Efectiv, orice abordare este folosită, la un anumit punct, vor trebui alocate bunuri pentru a implementa planurile de acțiune, şi inevitabil, justificarea pentru o astfel de investiție va fi pusă la îndoială.

Bunurile şi fondurile care vor fi alocate pentru securitate sunt, la fel ca şi pentru polițele de asigurare, în proporție directă cu riscul. Dacă nu există un acord comun asupra potențialului defecțiunilor, atunci este puțin probabil ca să fie alocat vreun buget.

### 2.2.3 Clasificare: un element esențial pentru politica de securitate

Cadrele de referință pentru securitate, politicile de securitate, şi abordarea asociată managementului securității au fost deja menționate în acest document.

În practică, companiile care administrează securitatea printr-un set de reguli sunt obligate să diferențieze, chiar în reguli, între acțiuni care vor fi efectuate ca o funcție a sensibilității informației care este procesată. Este obişnuit să se facă referire la o clasificare a informației şi a bunurilor sistemelor IT.

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

### 2.2.4 Analiza mizelor de securitate: baza planificării securității

Chiar procesul de analiză a mizelor de securitate, care necesită în mod evident contribuția managerilor operaționali, conduce foarte des la necesitatea pentru acțiune imediată.

Experiența arată că, atunci când managementul operațional de top a fost intervievat, indiferent de mărimea organizației, şi şi-au explicat punctul de vedere şi estimarea asupra defecțiunilor grave, acest lucru conduce la nevoi de securitate pe care nu le luaseră în considerare înainte şi care necesită răspunsuri rapide.

Planurile de acțiune pot fi apoi create direct, folosind o abordare uşoară şi directă bazată pe combinarea a două seturi de expertiză: aceea a profesiei înseşi, oferită de managementul operațional, şi cea a soluțiilor de securitate, oferită de experții în securitate.

## *2.3 Analiza riscului*

Analiza riscului este menționată în aproape toate publicațiile care privesc securitatea, ca fiind forța propulsoare în securitate. Totuşi, majoritatea nu discută metodele care trebuiesc folosite.

Pentru mai mult de zece ani, MEHARI a oferit o abordare structurată pentru evaluarea riscului[4], pe baza a câteva principii simple.

O situație de risc poate fi caracterizată de mai mulți factori:

- Factori structurali (sau organizaționali), care nu depind de măsuri de securitate, ci de activitatea de bază a organizației, de mediul său, şi de contextul acesteia.

[4] O descriere detaliată a modelului de risc este oferită în MEHARI Concepte Generale şi Mecanisme Principale

- Factori de reducere a riscului care sunt o funcție directă a măsurilor de securitate implementate.

MEHARI permite evaluarea calitativă şi cantitativă a acestor factori, şi ajută la evaluarea nivelurilor de risc ca rezultat.

De fapt, analiza mizelor de securitate este folosită pentru a determina un nivel de gravitate maxim al consecințelor unei situații de risc. Acest lucru este de obicei un factor structural, în timp ce evaluarea securității va fi folosită pentru a evalua factorii de reducere a riscului.

### 2.3.1 Analiza riscului: un ajutor în planificarea strategică

Identificarea factorilor de reducere a riscului, ei înşişi o funcție a măsurilor de securitate, oferă o bază metodologică pentru construirea unui plan de securitate sau a unui plan general strategic. Pentru a ajuta la acest lucru, MEHARI oferă o abordare structurată şi organizată pentru planificarea securității.

Abordarea este bazată pe o bază de cunoştințe a situațiilor de risc şi proceduri automate pentru evaluarea factorilor de reducere a riscului. În sprijinul abordării, o unealtă de software[5] scuteşte utilizatorul de la a trebui să facă calcule, şi oferă şi simulări şi optimizări.

Această utilizare a MEHARI se concentrează pe optimizarea globală a măsurilor de securitate cu scopul de a reduce riscurile.

### 2.3.2 Analiza sistematică a situațiilor de risc

Pe aceeaşi bază metodologică, o abordare uşor diferită este: să se identifice toate potențialele situații de risc, să se analizeze cele mai critice dintre ele, şi să se identifice acțiuni pentru a reduce riscul la un nivel acceptabil. MEHARI, sprijinit de bazele sale de cunoştințe, oferă pentru această abordare ceea ce trebuie.

Această utilizare a MEHARI se concentrează pe a se asigura că fiecare situație critică de risc a fost identificată şi este acoperită de un plan de acțiune.

### 2.3.3 Analiza spontană a situațiilor de risc

Acelaşi set de unelte poate fi folosit în orice moment în alte abordări de management al securității. În cazurile descrise deja, unde securitatea este administrată prin audituri sau cadre de referință pentru securitate, vor exista întotdeauna cazuri specifice unde regulile nu pot fi aplicate. Analiza spontană a riscului poate fi folosită pentru a decide cum este mai bine să se meargă mai departe.

### 2.3.4 Analiza riscului în proiecte noi

Modelul şi mecanismele de analiză a riscului pot fi folosite în managementul proiectelor, pentru a planifica împotriva riscului şi a decide ce măsuri ar trebui folosite ca rezultat.

## *2.4 Rezumat general al utilizărilor pentru MEHARI*

În mod clar, principala orientare a MEHARI o reprezintă analiza şi reducerea riscului. Bazele sale de cunoştințe, mecanismele şi uneltele au fost create pentru acel scop.

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

[5] Risicare, o unealtă de software, marcă înregistrată a BUC SA

- metodă de lucru permanentă – îndrumările pentru un grup specializat,
- metodă de lucru folosită în paralel cu alte practici de management al securității,
- metodă de lucru folosită ocazional pentru a completa practicile obişnuite.

Având în minte aceste lucruri, MEHARI oferă un set de abordări şi unelte care permit analizei riscului să fie efectuată atunci când este nevoie.

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

# 3 MEHARI şi standardele internaţionale

O întrebare care este deseori pusă este: cum corespunde MEHARI standardelor internaţionale – în special pentru ISO 13335, ISO17799[6] şi ISO/IEC 27001[7].

Aici, MEHARI nu va fi comparat direct cu standardele şi uneltele la care au dat naştere acestea. Intenţia este mai degrabă de a explica modul în care MEHARI se încadrează în standardele ISO, în ceea ce priveşte compatibilitatea scopurilor.

Standardul ISO 13335 include un model de management al riscului la care MEHARI face referire, şi cu care MEHARI este întru totul compatibil. MEHARI oferă o metodă şi unelte după cum este cerut de standard.

ISO 17799 şi ISO/IEC 27001 vor fi discutate aici cu privire la MEHARI.

## *3.1 Scopurile ISO 17799, ISO/IEC 27001 şi MEHARI*

### 3.1.1 Scopurile standardului ISO/IEC 17799:2005

Acest standard stipulează că o organizaţie ar trebui să-şi identifice cerinţele de securitate folosind trei surse principale:

- Analiza riscului,
- Cerinţele legale, statutare, sau contractuale,
- Setul de principii, scopuri, şi cerinţe care se aplică la procesarea informaţiilor pe care organizaţia l-a dezvoltat pentru a-i sprijini operaţiunile.

Folosind acest lucru drept bază, pot fi alese şi implementate puncte de control folosind lista oferită în secţiunea „codul de practică pentru managementul securităţii informaţionale" din standard sau din orice alt set de puncte de control (§4.2).

*NOTĂ: în scopul 17799:2005, se stipulează că standardul oferă „indicaţii şi principii generale pentru iniţierea, implementarea, întreţinerea şi îmbunătăţirea managementului securităţii informaţionale", ceea ce înseamnă că standardul ISO poate fi văzut ca un punct de pornire. Totuşi, ISO/IEC 27001 stipulează (§1.2) că orice excludere trebuie să fie justificată şi că este acceptabil să se adauge puncte de control (Anexa A – A.I).*

Standardul ISO 17799 oferă o compilaţie de indicaţii, pe care o organizaţie le poate folosi. Acesta notează totuşi, că lista nu este exhaustivă, şi că pot fi necesare măsuri complementare. Totuşi, nu este recomandată nici o metodologie pentru crearea unui sistem de management al securităţii complet.

Pe de altă parte, fiecare parte din ghidul cu cele mai bune practici include introducere şi comentarii despre scopurile vizate, ceea ce poate fi un ajutor foarte util.

[6] ISO/IEC 17799:2005(E)
[7] ISO/IEC 27001-2005

*NOTĂ: Standardul ISO stipulează în scopul său şi că poate fi folosit pentru „a ajuta la formarea încrederii în activităţi inter-organizaţionale". Acest lucru nu este inclus din întâmplare, şi scoate la iveală un aspect esenţial pe care cei care sprijină standardul îl promovează, şi anume evaluarea (chiar certificarea), din punctul de vedere al securităţii informaţionale, al partenerilor şi furnizorilor.*

### 3.1.2 Scopurile ISO/IEC 27001

Scopul clar al ISO/IEC 27001 este de a „oferi un model pentru a crea şi administra un **sistem de management al securităţii informaţionale** (ISMS) corporativ" şi de a fi „folosit fie intern sau de către terţi, inclusiv autorităţile de certificare".

Scopul de evaluare şi certificare pune o accentuare puternică pe aspectele formale (documentaţie şi înregistrarea deciziilor, declararea aplicabilităţii, registre, etc.) şi pe control (revizii, audituri, etc.).

Este clar că baza abordării de securitate implică că o analiză a riscului ar trebui efectuată, pentru a examina riscurile la care ar putea fi expusă o organizaţie, şi 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 folosită, dar acest lucru nu face parte din standard, şi nu este propusă nici o metodă anume, în afară de integrarea procesului recursiv PDCA (Planifică, Fă, Verifică, Acţionează) al modelului după cum este definit pentru crearea ISMS.

De asemenea, recomandările sau *cele mai bune practici* care pot fi folosite pentru a reduce riscul sunt „aliniate la cele enumerate în ISO/IEC 17799:2005", în timp ce este oferită o listă asociată cu puncte de control în anexe.

Potrivit ISO/IEC 27001, baza pentru **evaluarea sistemului de management al securităţii** nu este atât de mult cunoaşterea sau verificarea faptului dacă deciziile care au fost luate sunt corespunzătoare şi adaptate la nevoile organizaţiei, ci mai degrabă de a verifica că, odată ce deciziile au fost luate, sistemul de management este de aşa natură încât un auditor sau certificator poate fi sigur că deciziile au fost implementate cu adevărat.

### 3.1.3 Scopurile MEHARI

MEHARI reprezintă un set consecvent de unelte şi metode pentru managementul securităţii, bazat pe analiza riscului. Cele două aspecte fundamentale ale MEHARI: modelul său de risc (calitativ şi cantitativ) şi analiza riscului bazată pe modele de management al securităţii nu au componente echivalente nici în ISO/IEC 27001 nici în ISO 17799.

### 3.1.4 Compararea scopurilor MEHARI şi ale standardelor ISO 17799 şi ISO/IEC 27001

Scopurile MEHARI şi cele ale standardelor ISO menţionate mai sus sunt diferite radical.

- MEHARI ţinteşte să ofere unelte şi metode care pot fi folosite pentru a alege cele mai potrivite măsuri de securitate pentru o organizaţie dată. Acest lucru nu este cu siguranţă scopul declarat al nici unuia din standardele ISO.
- Standardele ISO oferă un set de cele mai bune practici, care sunt cu siguranţă foarte utile, dar nu neapărat potrivite pentru ceea ce este în joc în organizaţie, şi sunt utile pentru a acoperi aspectele maturităţii în securitate, planificarea securităţii informaţionale, auditurile interne independente şi partenerii.

Singurul punct din setul MEHARI care poate fi comparat cu ISO 17799 (şi Anexa A a ISO/IEC 27011)

este *manualul de referinţe pentru serviciile de securitate* al MEHARI. Acesta oferă eficient elemente detaliate care pot fi folosite pentru a clădi un cadru de securitate. La acest punct, este clar că acoperirea MEHARI este mai mare decât cea a ISO, şi că acoperă aspecte esenţiale ale securităţii trecând peste cele care ţin doar de sisteme informaţionale.

## *3.2 Compatibilitatea dintre aceste abordări*

Abordarea MEHARI este complet reconciliabilă cu ISO 17799 deoarece, deşi nu au aceleaşi obiective declarate, este relativ uşor să se reprezinte rezultatele unei analize MEHARI în ceea ce priveşte indicatorii ISO 17799.

MEHARI răspunde la necesitatea, exprimată în ambele standarde ISO, ca o analiză a riscului să definească măsurile care ar trebui implementate.

### 3.2.1 Compatibilitatea cu standardul ISO 17799

Punctele de control ale standardului sau *cele mai bune practici* ale ISO sunt în principal măsuri generale, comportamentale sau organizaţionale, în timp ce MEHARI accentuează necesitatea măsurilor tehnice ale căror eficienţă poate fi garantată. Rezultatele, în ceea ce priveşte managementul securităţii, vor fi radical diferite cu aceste două abordări.

În ciuda acestor diferenţe, recenzia vulnerabilităţi din MEHARI 2007 oferă tabele de corespondenţă pentru a arăta indicatorii aliniaţi la împărţirea folosită în standardul ISO 17799:2005, utilizabilă pentru cei care trebuie să dovedească conformarea la acel standard.

Merită menţionat faptul că aici chestionarele MEHARI pentru audit au fost concepute şi constituite astfel încât să permită managerilor operaţionali să efectueze treceri în revistă a vulnerabilităţilor în mod eficient şi să deducă capacitatea fiecărui serviciu de securitate pentru a reduce aceste riscuri.

### 3.2.2 Compatibilitatea cu standardul ISO 27001

MEHARI poate fi integrat cu uşurinţă în procesul ISO/IEC 27001, mai ales în faza „PLANIFICĂ” (§4.2.1). MEHARI acoperă complet descrierea sarcinilor care permit crearea bazelor ISMS.

Pentru faza „FĂ” (§4.2.2), care ţinteşte să implementeze şi să administreze ISIS, MEHARI oferă elemente de pornire utile precum construirea planurilor pentru managementul riscului, cu prioritizarea legată direct de clasificarea riscului, şi măsurarea progresului în timpul utilizării lor. Pentru faza „VERIFICĂ” (§4.2.3), MEHARI oferă elemente care permit evaluarea riscurilor reziduale, şi măsurătorile realizate în măsurile de securitate. În plus, orice modificări la mediu (mizele, ameninţările, soluţiile şi organizaţia) pot fi reevaluate cu uşurinţă prin audituri vizate care folosesc rezultatele auditului MEHARI iniţial. Astfel, planurile de securitate pot fi revizuite şi pot evolua în timp.

Pentru faza „ACŢIONEAZĂ” (§4.2.4), MEHARI recurge implicit la controale şi îmbunătăţirea continuă a securităţii; asigurând astfel că scopurile de reducere a riscurilor sunt atinse. În aceste trei faze, deşi MEHARI nu se află în mijlocul proceselor, el contribuie mult la executarea lor şi asigură eficienţa lor.