



MEHARI 2007

Privire Generală

MEHARI este marcă înregistrată a CLUSIF

Recunoaștere

CLUSIF dorește să mulțumească membrilor echipei de lucru care au contribuit la crearea acestui document.

CLUSIF dorește de asemenea să mulțumească dlui. Valentin P. Măzăreanu și echipei sale (Alina Marin, Raluca Ungureanu) care au acceptat să furnizeze această traducere. Dl. Valentin P. Măzăreanu își desfășoară activitatea în cadrul Facultății de Economie și Administrarea Afacerilor, Universitatea „Al.I.Cuza” Iași și este director general al Paideia Consulting Iași. Pentru mai multe informații despre activitatea dlui. Valentin P. Măzăreanu vă invităm să accesați www.managementul-riscurilor.ro.

Vă rugăm să trimiteți întrebările și comentariile dumneavoastră la adresa mehari@clusif.asso.fr

Cuprins

1	Introducere	4
2	Utilizări ale Mehari	5
2.1	Evaluările de securitate	6
2.1.1	Recenzia vulnerabilității, un element al analizei riscului	6
2.1.2	Planuri de securitate pe baza trecerilor în revistă ale vulnerabilităților	6
2.1.3	Sprijin oferit de bazele de cunoștințe în crearea unui cadru de referință pentru securitate	7
2.1.4	Domenii acoperite de modulul de evaluare	7
2.1.5	Rezumat al modulului de evaluare	7
2.2	Analizarea mizelor	7
2.2.1	Analizarea mizelor, baza pentru o analiză a riscului	8
2.2.2	Analiza mizelor de securitate: piatra de temelie pentru orice planificare de acțiune strategică	9
2.2.3	Clasificare: un element esențial pentru politica de securitate	9
2.2.4	Analiza mizelor de securitate: baza planificării securității	9
2.3	Analiza riscului	9
2.3.1	Analiza riscului: un ajutor în planificarea strategică	10
2.3.2	Analiza sistematică a situațiilor de risc	10
2.3.3	Analiza spontană a situațiilor de risc	10
2.3.4	Analiza riscului în proiecte noi	10
2.4	Rezumat general al utilizărilor pentru MEHARI	10
3	MEHARI și standardele internaționale	12
3.1	Scopurile ISO 17799, ISO/IEC 27001 și MEHARI	12
3.1.1	Scopurile standardului ISO/IEC 17799:2005	12
3.1.2	Scopurile ISO/IEC 27001	13
3.1.3	Scopurile MEHARI	13
3.1.4	Compararea scopurilor MEHARI și ale standardelor ISO 17799 și ISO/IEC 27001	13
3.2	Compatibilitatea dintre aceste abordări	14
3.2.1	Compatibilitatea cu standardul ISO 17799	14
3.2.2	Compatibilitatea cu standardul ISO 27001	14

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 și pentru auditorii sau managerii de risc care se confruntă în mare cu aceleași 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 și a uneltelor asociate este oferită în alte documente disponibile de la Clusif, în special:

- *MEHARI: Concepte și Mecanisme*
- *MEHARI: Analiza mizelor și Ghidul de clasificare*
- *MEHARI: Ghidul de evaluare pentru serviciile de securitate*
- *MEHARI: Ghidul Analizei Riscului*
- *MEHARI: Baze de cunoștințe și Manuale cu referințe (servicii de securitate și scenarii de risc).*

MEHARI dorește 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”,
- Desfășurarea evaluărilor ușoare sau detaliate a stării securității,
- Evaluarea și managementul riscului,
- Asigurarea includerii securității în managementul proiectelor aflate în dezvoltare,
- Conștientizarea securității și sesiuni de training,
- Managementul operațional al securității și controlul/monitorizarea acțiunilor săvârșite.

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

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

- Maturitatea, în ceea ce privește securitatea, a organizației și a personalului său,
- Nivelul de implicare a conducerii în luarea deciziilor în securitatea informațională,
- Cultura întreprinderii: ierarhică și tehnocrată (regulile există și sunt aplicate), sau, dimpotrivă, descentralizată și 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 și complementare între ele, permițând mișcarea de la una la alta fără duplicarea sarcinilor sau muncă suplimentară.

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

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

2 Utilizări ale Mehari

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

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

În termeni de zi cu zi, managementul securității este o funcție sau activitate care evoluează în timp. Acțiunile manageriale 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.

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

După această evaluare a stării și decizia de a implementa securitatea organizațională, se vor decide acțiunile concrete. Astfel de decizii, care vor fi grupate de obicei în planuri, reguli ale corporației, politici sau un cadru de referință al securității, ar trebui luate folosind o abordare structurată. Această abordare se poate baza pe analiza riscului, sau poate include conceptul de risc, deși nu este obligatoriu. 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?”. Datorită 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 începutului unei abordări de securitate, riscul real pe care organizația sau întreprinderea și-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 organizația ar putea fi expusă, și există o oarecare asigurare că nivelurile acestora sunt acceptabile?”. Această întrebare ar putea la fel de ușor să fie adresată la nivelul corporației, 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 securității trebuie să fie consecvente. Prin asta, se poate înțelege că orice rezultate generate la un anumit stadiu trebuie să fie reutilizabile de alte unelte mai târziu sau în altă parte în organizație.

Diferitele unelte și module a setului de metodologie MEHARI, concepute pentru a însoți analiza riscului, pot fi folosite separat una de cealaltă la orice pas al dezvoltării securității, folosind diferite abordări de management, și pot garanta o consecvență a deciziilor care rezultă.

Toate aceste unelte și module – descrise pe scurt mai jos – cuprind unelte pentru evaluarea stării securității, un modul pentru analizarea mizelor, și 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 rapidă¹
- 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 aceleași 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, și apoi să repete în profunzime în orice moment, și pentru orice punct care poate necesita asigurare. Modulele de evaluare pot fi folosite în mai multe moduri².

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 ști 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 își 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 și decide să îmbunătățești toate acele servicii care nu au un nivel al calității suficient de bun.

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

Stadiile diferite și 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
Privire generală

2.1.3 Sprijin oferit de bazele de cunoștințe în crearea unui cadru de referință pentru securitate

Modulul de evaluare detaliată utilizează baza de cunoștințe a serviciilor de securitate (documentată în *MEHARI – manualul de referințe pentru servicii de securitate*³). Acesta descrie, pentru fiecare serviciu, la ce folosește, împotriva a ce este folosit, mecanismele și soluțiile care sprijină serviciul, și acele elemente care ar trebui considerate atunci când se evaluează calitatea serviciului.

Această bază de cunoștințe unică poate fi folosită direct pentru a crea un cadru de referință pentru securitate (sau politici de securitate) care va conține, și va descrie, setul de reguli și instrucțiuni de securitate pe care întreprinderea sau organizația le va urma.

Această abordare este deseori folosită în organizații sau întreprinderi cu mai multe unități sau site-uri operaționale independente. Acesta ar fi de obicei cazul pentru companiile multinaționale mari cu mai mulți afiliați; dar se aplică la fel de ușor pentru companiile medii cu un număr mare de filiale sau agenții regionale. În astfel de cazuri, este greu să se efectueze numeroase evaluări sau analize ale riscului.

Construirea cadrului de referință al securității

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

Administrarea excepțiilor de la regulă

Crearea unui set de reguli, printr-un cadru de referință pentru securitate, intră deseori în conflict cu dificultățile de implementare locale; așa că, trebuiesc administrate abandonuri și excepții de la reguli.

Utilizarea unei baze de cunoștințe coerente, cu un set de unelte consecvent și o metodologie analitică, permite administrarea divergențelor locale. Cererile pentru excepții 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 privește toate situațiile de risc și dorința de a acoperi toate riscurile inacceptabile, MEHARI nu este restricționat doar la domeniul IT.

Modulul de evaluare acoperă, în afară de sistemul informațional, organizația în ansamblu, și protecția site-ului în general, precum și mediul de lucru și aspectele legale și reglementatoare.

2.1.5 Rezumat al modulului de evaluare

Lucrul care trebuie reținut în legătură cu modulul de evaluare este că oferă o privire largă și consecventă asupra securității. Acest lucru poate fi folosit în mai multe abordări, care evoluează în ceea ce privește profunzimea și granulozitatea analizei, și poate fi folosit în toate stadiile de maturitate ale conștientizării securității întreprinderii și a organizației.

2.2 Analizarea mizelor

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

³ Manualul de referințe pentru serviciile de securitate face parte din bazele de cunoștințe 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 și importanța mizelor de securitate în sine.

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

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

„Ce s-ar putea întâmpla, și 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 și clasificare*, care produce două tipuri de rezultate:

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

Scara de valori a 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. 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 și a bunurilor

Este ceva obișnuit, în securitatea sistemului IT, să se vorbească despre clasificarea informației și despre clasificarea bunurilor IT.

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

Clasificarea informației și 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 și clasificarea informației și a bunurilor reprezintă două moduri distincte de a exprima mizele de securitate.

Prima este mai detaliată și oferă mai multe informații pentru CISO. Cea din urmă este mai globală și mai utilă pentru campaniile de conștientizare și 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, și inevitabil, justificarea pentru o astfel de investiție va fi pusă la îndoială.

Bunurile și fondurile care vor fi alocate pentru securitate sunt, la fel ca și 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

Cadrelor de referință pentru securitate, politicile de securitate, și 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 obișnuit să se facă referire la o clasificare a informației și 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, și și-au explicat punctul de vedere și estimarea asupra defecțiunilor grave, acest lucru conduce la nevoi de securitate pe care nu le luaseră în considerare înainte 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 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. Totuși, majoritatea nu discută metodele care trebuiesc folosite.

Pentru mai mult de zece ani, MEHARI a oferit o abordare structurată pentru evaluarea riscului⁴, 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, și de contextul acesteia.

⁴ O descriere detaliată a modelului de risc este oferită în MEHARI Concepte Generale și Mecanisme Principale
Privire generală

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

MEHARI permite evaluarea calitativă și cantitativă a acestor factori, și 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 înșiși 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 și organizată pentru planificarea securității.

Abordarea este bazată pe o bază de cunoștințe a situațiilor de risc și proceduri automate pentru evaluarea factorilor de reducere a riscului. În sprijinul abordării, o unealtă de software⁵ scutește utilizatorul de la a trebui să facă calcule, și oferă și simulări și 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 aceeași bază metodologică, o abordare ușor diferită este: să se identifice toate potențialele situații de risc, să se analizeze cele mai critice dintre ele, și să se identifice acțiuni pentru a reduce riscul la un nivel acceptabil. MEHARI, sprijinit de bazele sale de cunoștințe, 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 și este acoperită de un plan de acțiune.

2.3.3 Analiza spontană a situațiilor de risc

Același 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 și mecanismele de analiză a riscului pot fi folosite în managementul proiectelor, pentru a planifica împotriva riscului și 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 și reducerea riscului. Bazele sale de cunoștințe, mecanismele și uneltele au fost create pentru acel scop.

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

⁵ Risicare, o unealtă de software, marcă înregistrată a BUC SA
Privire generală

- 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 obișnuite.

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

Metodologia MEHARI, cuprinzând bazele de cunoștințe, manualele și 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 și acțiuni.

3 MEHARI și standardele internaționale

O întrebare care este deseori pusă este: cum corespunde MEHARI standardelor internaționale – în special pentru ISO 13335, ISO17799⁶ și ISO/IEC 27001⁷.

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

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

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

3.1 Scopurile ISO 17799, ISO/IEC 27001 și MEHARI

3.1.1 Scopurile standardului ISO/IEC 17799:2005

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

- Analiza riscului,
- Cerințele legale, statutare, sau contractuale,
- Setul de principii, scopuri, și cerințe care se aplică la procesarea informațiilor pe care organizația l-a dezvoltat pentru a-i sprijini operațiunile.

Folosind acest lucru drept bază, pot fi alese și implementate puncte de control folosind lista oferită în secțiunea „codul de practică pentru managementul securității informaționale” din standard sau din orice alt set de puncte de control (§4.2).

NOTĂ: în scopul 17799:2005, se stipulează că standardul oferă „indicații și principii generale pentru inițierea, implementarea, întreținerea și îmbunătățirea managementului securității informaționale”, ceea ce înseamnă că standardul ISO poate fi văzut ca un punct de pornire. Totuși, ISO/IEC 27001 stipulează (§1.2) că orice excludere trebuie să fie justificată și că este acceptabil să se adauge puncte de control (Anexa A – A.I).

Standardul ISO 17799 oferă o compilație de indicații, pe care o organizație le poate folosi. Acesta notează totuși, că lista nu este exhaustivă, și că pot fi necesare măsuri complementare. Totuși, nu este recomandată nici o metodologie pentru crearea unui sistem de management al securității complet.

Pe de altă parte, fiecare parte din ghidul cu cele mai bune practici include introducerea și 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 și că poate fi folosit pentru „a ajuta la formarea încrederii în activități inter-organizaționale”. Acest lucru nu este inclus din întâmplare, și scoate la iveală un aspect esențial pe care cei care sprijină standardul îl promovează, și anume evaluarea (chiar certificarea), din punctul de vedere al securității informaționale, al partenerilor și furnizorilor.

3.1.2 Scopurile ISO/IEC 27001

Scopul clar al ISO/IEC 27001 este de a „oferi un model pentru a crea și administra un **sistem de management al securității informaționale** (ISMS) corporativ” și de a fi „folosit fie intern sau de către terți, inclusiv autoritățile de certificare”.

Scopul de evaluare și certificare pune o accentuare puternică pe aspectele formale (documentație și înregistrarea deciziilor, declararea aplicabilității, registre, etc.) și 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 organizație, 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 folosită, dar acest lucru nu face parte din standard, și nu este propusă nici o metodă anume, în afară de integrarea procesului recursiv PDCA (Planifică, Fă, Verifică, Acționează) 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 „aliniată 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 securității** nu este atât de mult cunoașterea sau verificarea faptului dacă deciziile care au fost luate sunt corespunzătoare și adaptate la nevoile organizației, ci mai degrabă de a verifica că, odată ce deciziile au fost luate, sistemul de management este de așa natură încât un auditor sau certficator poate fi sigur că deciziile au fost implementate cu adevărat.

3.1.3 Scopurile MEHARI

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

3.1.4 Compararea scopurilor MEHARI și ale standardelor ISO 17799 și ISO/IEC 27001

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

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

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

este *manualul de referință 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, și că acoperă aspecte esențiale ale securității trecând peste cele care țin doar de sisteme informaționale.

3.2 Compatibilitatea dintre aceste abordări

Abordarea MEHARI este complet reconciliabilă cu ISO 17799 deoarece, deși nu au aceleași obiective declarate, este relativ ușor să se reprezinte rezultatele unei analize MEHARI în ceea ce privește 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 organizaționale, în timp ce MEHARI accentuează necesitatea măsurilor tehnice ale căror eficiență poate fi garantată. Rezultatele, în ceea ce privește managementul securității, vor fi radical diferite cu aceste două abordări.

În ciuda acestor diferențe, recenzia vulnerabilități din MEHARI 2007 oferă tabele de corespondență pentru a arăta indicatorii aliniați la împărțirea folosită în standardul ISO 17799:2005, utilizabilă pentru cei care trebuie să dovedească conformarea la acel standard.

Merită menționat faptul că aici chestionarele MEHARI pentru audit au fost concepute și constituite astfel încât să permită managerilor operaționali să efectueze treceri în revistă a vulnerabilităților în mod eficient și 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 ușurință 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 țintește să implementeze și să administreze ISIS, MEHARI oferă elemente de pornire utile precum construirea planurilor pentru managementul riscului, cu prioritizarea legată direct de clasificarea riscului, și măsurarea progresului în timpul utilizării lor. Pentru faza „VERIFICĂ” (§4.2.3), MEHARI oferă elemente care permit evaluarea riscurilor reziduale, și măsurătorile realizate în măsurile de securitate. În plus, orice modificări la mediu (mizele, amenințările, soluțiile și organizația) pot fi reevaluate cu ușurință prin audituri 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 recurge implicit la controale și îmbunătățirea continuă a securității; asigurând astfel că scopurile de reducere a riscurilor sunt atinse. În aceste trei faze, deși MEHARI nu se află în mijlocul proceselor, el contribuie mult la executarea lor și asigură eficiența lor.