



MEHARI 2007

Ghid de evaluare pentru serviciile de securitate

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	Construirea unei scheme de audit	5
2.1	Scopul unei scheme de audit	5
2.2	Construirea unei scheme de audit	5
2.2.1	Domeniile MEHARI de responsabilitate	6
2.2.2	Tipuri de sub-seturi care ar trebui personalizate pentru audite de securitate	6
2.2.3	Crearea unei scheme de audit detaliate	7
2.2.4	Construirea schemelor de audit specifice	8
3	Procesul de recenzie	9
3.1	Evaluarea calității serviciului de securitate	9
3.1.1	Parametri obligatorii	9
3.1.1.1	Eficiența serviciului de securitate	9
3.1.1.2	Cât de robust este un serviciu de securitate?	10
3.1.1.3	Permanența	10
3.1.2	Definiția calității nivelelor serviciului de securitate	10
3.2	Evaluarea directă a calității serviciului de securitate	11
3.3	Evaluarea calității serviciului de securitate folosind chestionare MEHARI	11
3.3.1	Tipuri de chestionare	12
3.3.2	Sistemul de evaluare	12
3.3.2.1	Măsuri contributive	12
3.3.2.2	Măsuri majore sau „suficiente”	13
3.3.2.3	Măsuri esențiale	14
3.3.2.4	Întrebări inaplicabile	15
3.4	Procesul de audit	15
3.4.1	Procesul de revizie	15
3.4.2	Notarea și corectarea notării	16
4	Produse livrabile	18
4.1	Graficul sintetic al serviciului de securitate	18
4.2	Graficul sintetic „tematic”	18
4.3	Măsuri de concordanță legate de standardul ISO 17799:2005	18
5	Sfaturi practice	20
5.1	Puncte importante care trebuie incluse în schemele de audit	20
5.2	Puncte importante care trebuie acoperite în procesul de audit	20

1 Introducere

O privire generală asupra principiilor unei recenzii a vulnerabilității este oferită în documentul „Concepte și Mecanisme”. Principalele puncte sunt amintite mai jos.

Acest document examinează procesul de evaluare și oferă mai multe detalii complementare care pot fi necesare.

Pe scurt, recenzia MEHARI a vulnerabilității, sau auditul securității, constă în:

- O schemă de audit a diferite domenii de securitate, fiecare dintre ele trebuind analizat separat.
- O re-evaluare a serviciilor de securitate pentru reducerea riscului, pentru fiecare domeniu. Acest lucru ar trebui să acopere eficiența și robustețea fiecărui serviciu, și modul în care este supravegheat operațional. Această evaluare este făcută de obicei prin chestionare, dar poate fi realizată și direct.
- O privire generală asupra vulnerabilităților reziduale.

În teorie, recenzia vulnerabilității privește un set comprehensiv de servicii de securitate, care ar trebui deci identificat în avans. Presupunerea noastră, pentru restul acestui document, este că serviciile care vor fie examinate de recenzia vulnerabilității sunt cele definite în baza de cunoștințe MEHARI a serviciilor de securitate.

2 Construirea unei scheme de audit

Serviciile de securitate, așa cum sunt ele definite de MEHARI, reprezintă funcții de securitate, care sunt oferite de **soluții** implementate în întreprindere sau organizație.

Recenzia vulnerabilității implică, în practică, analiza și auditul soluțiilor și procedurilor implementate pentru a asigura funcțiile de securitate.

Totuși, există de obicei un număr de soluții care asigură un tip de protecție dat.

De exemplu, controlul accesului fizic la premise este în mod sigur oferit de diferite mecanisme și soluții – iar acestea vor fi diferite pentru accesul în camera calculatoarelor, sau alte centre tehnice, precum instalațiile PABX, camerele de conferință, și instalațiile electrice mari.

Este de asemenea evident că controlul accesului logic la diferite sisteme (mainframe-uri, UNIX, NT, și așa mai departe) va fi administrat în moduri diferite în funcție de tipul și nivelul sensibilității sistemului.

Înainte chiar de a ne gândi la procesul de analiză și evaluare a serviciilor de securitate, CISO sau auditorul de securitate ar trebui să identifice mai întâi care soluții specifice ar trebui analizate și auditate. În MEHARI acest lucru este numit „**planul de audit**” sau „**schema de audit**”.

2.1 Scopul unei scheme de audit

Într-o lume ideală, fiecare serviciu de securitate în parte ar trebui examinat, și toate soluțiile care oferă aceste servicii în organizație ar trebui identificate, astfel încât să poată fi auditate individual.

Acest lucru ar conduce la o cantitate de muncă incredibil de mare pentru un rezultat al cărui nivel al detaliului ar fi de prisos. Simplificarea este, de aceea, recomandată prin gruparea serviciilor asemănătoare astfel încât să poată fi analizate ca seturi omogene.

Totuși, nu este de obicei posibil să se ia în considerare ca echivalente toate soluțiile implementate în întreprindere. Acest lucru ar fi ca și cum s-ar considera că toate clădirile și camerele sunt protejate în același fel, că toate părțile infrastructurii IT au aceleași planuri de rezervă, sau că toate datele sunt depozitate și au back up în același mod. Evident, nu este cazul.

Este, desigur, întotdeauna posibil să se grupeze diferite obiecte într-un singur set, care ar fi apoi luat în considerare ca un întreg omogen. Dar ar trebui observat faptul că o recenzie precaută a vulnerabilității poate aplica cea mai pesimistă evaluare tuturor obiectelor unui set dat. Acest lucru ar oferi o percepție generală foarte slabă asupra întregului set.

Trebuie, de aceea, să găsim o cale de mijloc. Acest lucru ne va permite să diferențiem între mai multe soluții ale domeniilor care ar trebui auditate separat, și în cadrul cărora soluțiile de securitate pot fi considerate omogene. Definiția acestor domenii este reprezentată de către „schema de audit”.

2.2 Construirea unei scheme de audit

Abordarea MEHARI este să ia în considerare faptul că serviciile de securitate sunt definite și implementate de către echipe de dimensiuni limitate, cu o politică de securitate (fie că este documentată explicit sau nu) care îi va face să ia decizii omogene și consecvente, chiar și atunci când constrângerile tehnice necesită soluții care diferă în detalii.

Pe această bază, principiile MEHARI sunt să:

- Facă distincția între domenii de responsabilitate unde o persoană poate fi clar definită ca având **responsabilitatea pentru un domeniu care are o politică de securitate consecventă**.
- Să analizeze, în cadrul acestor domenii, dacă există diferite persoane care ar putea avea politici de securitate diferite, și astfel să definească diferite sub-domenii de responsabilitate. De exemplu, administratorii de site pot avea, pentru securitatea site-ului lor, politici care sunt diferite de cele ale altui site.
- Să analizeze, în fiecare domeniu sau sub-domeniu, **sub-seturile care pot avea politici diferite din oricare motiv (tehnic sau altul)**.

2.2.1 Domeniile MEHARI de responsabilitate

MEHARI definește domeniile de responsabilitate, numerotate de la 1 la 12, care, din punct de vedere al securității, acoperă:

- Organizația
- Securitatea fizică a site-ului
- Securitatea fizică a clădirilor și camerelor
- Arhitectura și nivelele de continuitate ale serviciului ale rețelelor extinse inter-site
- Arhitectura și nivelele de continuitate ale serviciului rețelelor locale
- Operarea rețelei
- Arhitectura sistemelor și securitatea logică
- Operarea sistemelor IT
- Securitatea aplicațiilor
- Dezvoltarea IT
- Spațiul de lucru, și mediul de lucru general
- Aspecte legale și aplicarea reglementărilor sau directivelor

Finalitatea schemei de audit este de a defini audite specifice pentru fiecare domeniu. Chestionarele de audit MEHARI sunt chiar și ele împărțite urmând această organizare. Ele sunt organizate în acest mod pentru a optimiza procesul de audit.

Primul nivel structural al schemei de audit va reflecta deci această descompunere. Apoi auditorul va trebui să decidă, pentru fiecare domeniu care este acoperit, câte variații ar trebui definite:

- Câte organizații diferite ar trebui auditate separat pentru funcțiile de securitate care depind de organizație?
- Câți administratori de site pot avea o politică de securitate specifică, care necesită recenzii ale vulnerabilității separate?
- Câți administratori locali ai premisei pot avea o politică de securitate specifică, care necesită recenzii ale vulnerabilității separate?
- Există mai mulți administratori de rețea locală care ar trebui să fie intervievați separat?
- Și așa mai departe.

De fiecare dată când există nevoia de a se distinge între entități sau responsabilități (din motive de autonomie, sau din imposibilitatea de a aplica politici consecvente), ar trebui create sub-domenii, și multiplicare chestionarele pentru fiecare dintre ele.

2.2.2. Tipuri de sub-seturi care ar trebui personalizate pentru audite de securitate

Al doilea nivel al descompunerii schemei de audit tratează strategiile tehnice, sau alte motive care necesită diferențierea, în cadrul fiecărui domeniu, între sub-seturi care ar putea necesita politici de securitate specifice. Tipul de întrebări care ar trebui puse la acest nivel este:

- Câte tipuri diferite de organizații trebuie auditate separat pentru funcțiile de securitate care depind de organizație?
- Câte tipuri diferite de site au o politică de securitate specifică, recenzii de vulnerabilitate (centrale chimice, locații cu acorduri de apărare specifice, care se ocupă cu detalii personale, sociale sau ale impozitelor, și așa mai departe)?
- Câte tipuri de premise ar trebui diferențiate în planul de securitate (birouri, camere ale computerelor, centre tehnice, și așa mai departe)?
- Câte rețele extinse inter-site și externe (internet, de exemplu)?
- Câte tipuri de rețele locale?
- Etc.

Pentru fiecare domeniu, va trebui să identificați câte variații diferite trebuie identificate și auditate individual.

2.2.3 Crearea unei scheme de audit detaliate

Schema de audit reprezintă rezultatul acestor două componente structurale: domeniile de responsabilitate pe de o parte, și variațiile personalizate pe de altă parte.

O schemă de audit globală a corporației care reprezintă rezultatul acestei abordări ar putea să redea de obicei un tabel de tipul celui arătat mai jos:

Domeniu	Sub-domenii (exemple)	Tipuri de sub-domenii
Organizație	Lipsă (fără descompunere)	Întreaga întreprindere
Locații	Sediul central și agențiile de vânzări Fabrici (administrare de departamentul de producție industrială)	Sediul central Agenții de vânzări Locații pentru producție
Premise	Birouri și alte premise conduse de departamentul central al lucrărilor. Domenii IT, electrice, tehnice și al telecomunicațiilor	Zone conduse de părți terțe (ex. racordul la energie electrică) Camere ale computerelor Alte zone tehnice
Arhitectura rețelei extinse	Nici una (fără descompunere)	Rețeaua inter-site extinsă
Arhitectura rețelei locale	Rețele IT Rețele ale proceselor de producție (administrare de departamentul de producție industrială)	Rețele IT Rețele ale proceselor de producție
Operarea rețelei	Rețele IT Rețele ale proceselor de producție (administrare de departamentul de producție industrială)	Rețele IT Rețele ale proceselor de producție

Sisteme	Sisteme IT Sisteme ale proceselor de producție (administrare de departamentul de producție industrială)	Mainframe-uri Sisteme deschise (Unix & NT) Sisteme de management a procesului Sisteme de management al securității procesului
Operarea sistemelor IT	Sisteme IT Sisteme ale procesului de producție (administrare de departamentul de producție industrială)	Mainframe-uri Sisteme deschise (Unix & NT) Sisteme de management a procesului
Securitatea aplicațiilor	Nici una (fără descompunere)	Aplicații mainframe Aplicații ale sistemelor deschise
Dezvoltarea IT	Dezvoltarea condusă de departamentul IT Dezvoltarea specifică executată de utilizatori	Dezvoltarea condusă de departamentul IT Dezvoltarea specifică executată de utilizatori
Mediul de lucru	Sediul central și puncte de vânzare Fabrici (administrare de departamentul de producție industrială)	Sediul central Puncte de vânzare Fabrici de producție
Mediul legal și respectarea directivelor	Legislația națională și reglementările și directivele în vigoare	Statutul legal al întreprinderii

O astfel de schemă de audit permite definirea unei organizări detaliate pentru recenzia de vulnerabilitate, și identificarea necesității pentru o recenzie specifică a vulnerabilității pentru fiecare din obiectele trecute în coloana din dreapta. Auditorul de securitate poate deci multiplica chestionarul (dacă se folosesc chestionare) în atâtea copii câte domenii sunt în domeniul corespondent.

2.2.4 Construirea schemelor de audit specifice

Este, desigur, posibil să se construiască scheme de audit specifice care să corespundă nevoilor specifice și care nu acoperă toate domeniile.

Este posibil, de exemplu, să se construiască o schemă de audit specifică pentru un departament sau un proiect (de la mediul de lucru al utilizatorului prin sistemele și aplicațiile folosite). Acest lucru s-ar realiza prin selectarea domeniilor în discuție și conectarea sub-seturilor corespunzătoare cu zonele în discuție.

3 Procesul de recenzie

3.1. Evaluarea calității serviciului de securitate

Această sub-sectiune face rezumatul aspectelor fundamentale deja descrise în „*Concepte și Mecanisme*”. Cititorii care sunt deja bine versați în aceste principii ar trebui să treacă direct la sub-sectiunea 3.2.

Serviciile de securitate pot varia în performanță. Acestea vor fi mai mult sau mai puțin eficiente în funcția lor, și mai mult sau mai puțin robuste în capacitatea lor de a rezista atacurilor directe, în funcție de mecanismele folosite și de aspectele organizaționale.

3.1.1 Parametri obligatorii

Pentru a măsura performanța serviciului de securitate, trebuie luați în considerare mai mulți parametri:

- Eficiența
- Robustețea
- Permanența.

3.1.1.1 Eficiența serviciului de securitate

Pentru serviciile de natură tehnică, eficiența este o măsură a capacității lor de a asigura eficient funcția necesară atunci când se confruntă cu un personal mai mult sau mai puțin competent sau cu circumstanțe mai mult sau mai puțin obișnuite.

Să luăm, ca exemplu, sub-serviciul „Managementul autorizării accesului la sisteme informaționale”, care implică atribuirea drepturilor de acces ale utilizatorilor. Funcția acestui serviciu este de a asigura că doar acele persoane care au autorizația managementului lor primesc accesul corespunzător la sistemele informaționale. În practică, eficiența serviciului depinde de strictețea controalelor, de autenticitatea cererii, și de corelarea relației ierarhice dintre petiționar și noul utilizator. Dacă tot ce se cere este o simplă trimitere poștală, fără semnătură sau certificat, oricine cunoaște câte ceva despre procesul de autorizare ar putea să își aloce singuri fără permisiune drepturi de acces, și calitatea sub-serviciului ar fi considerată ca fiind slabă.

Eficiența unui serviciu care administrează acțiunile umane reprezintă astfel măsura competenței necesare pentru a permite unor persoane să treacă de controalele în vigoare, sau chiar să abuzeze de ele.

Pentru acele servicii care tratează evenimentele naturale (*precum detectarea incendiilor, stingerea incendiilor*), eficiența reprezintă o măsură a „puterii” evenimentului pentru care intervenția lor rămâne eficientă.

Dacă acest lucru privește, de exemplu, un baraj care trebuie să împiedice un râu să se reverse din cauza ploilor abundente, eficiența este direct legată de debitul apei (puterea inundației) căreia i se opune. În practică, puterea va fi deseori măsurată ca o funcție a caracterului excepțional al evenimentului.

Serviciile care oferă acoperire generală nu pot, în principiu, să fie evaluate pe baza efectului lor direct, ci doar pe baza rolului lor indirect.

Eficiența măsurilor generale reprezintă rezultatul capacității lor de a crea planuri de acțiune sau

schimbări de comportament semnificative.

3.1.1.2 Cât de robust este un serviciu de securitate?

Robustețea unui serviciu de securitate măsoară capacitatea sa de a rezista unei acțiuni care este menită să scurt-circuiteze serviciul, sau să-i restricționeze eficiența.

Robustețea privește doar acele servicii care sunt considerate tehnice.

În exemplul precedent (managementul accesului), robustețea sub-serviciului depinde – în mod deosebit – de cât de ușor este să se acceseze direct tabelul cu drepturile de acces ale utilizatorilor, și astfel să se permită cuiva să își atribuie drepturi de acces fără necesitatea de a urma procesele de control obișnuite.

Atunci când avem de-a face cu servicii pentru managementul accidentelor sau al evenimentelor naturale (precum detectarea incendiilor, stingerea automată a incendiilor, și așa mai departe), robustețea lor va acoperi și capacitatea de a evita să fie scurt-circuitate sau evitate (fie accidental, sau intenționat).

3.1.1.3 Permanența

Calitatea globală a unui serviciu de securitate necesită ca serviciul să fie garantat în timp.

Pentru aceasta, orice întrerupere a serviciului poate fi detectată și pot fi aplicate măsuri paliative. Totul depinde, de aceea, de viteza detectării și de capacitatea de a reacționa.

Pentru măsurile generale, supravegherea soluțiilor este importantă pentru a arăta că acestea pot fi măsurate cu adevărat, în ceea ce privește implementarea și eficacitatea, dar și că există indicatori ai calității efective a serviciului și puncte de control implementate.

3.1.2 Definiția calității nivelelor serviciului de securitate

Calitatea unui serviciu de securitate măsoară eficiența sa, cât de robust este, și existența controalelor obișnuite. Global, de aceea, calitatea unui serviciu de securitate reprezintă capacitatea sa de a rezista oricărui atac asupra măsurilor sale de apărare - deși nici un castel nu poate fi considerat a fi de necucerit.

Calitatea serviciului de securitate este notată pe o scară de la 0 la 4. Această scară reflectă competența sau hotărârea care este necesară pentru a trece de apărare, pentru a o scurt-circuita, sau pentru a împiedica sau face inutilă detectarea neutralizării serviciului.

Deși această scară de valori permite valori fracționale, credem că este util să se indice valorile întregi pentru un serviciu de securitate.

Calitatea serviciului evaluat de nivelul 1

Acest serviciu are un nivel minim. Ar putea fi total inefficient (sau nu rezistă) când se confruntă cu un utilizator obișnuit, fără calificări deosebite, sau puțin ducut. În evenimentele naturale, este probabil să nu fie de nici un folos în problemele de zi cu zi. În general, va avea un efect mic sau deloc asupra comportamentului sau eficienței organizației.

Calitatea serviciului evaluat ca fiind de nivelul 2

Serviciul este de obicei eficient și rezistă unui hacker mediu sau puțin competent. Totuși, el este cu siguranță insuficient atunci când se confruntă cu un profesionist cu experiență în acel domeniu (acesta ar putea fi un profesionist IT, un hoț bine echipat, sau un expert în spargeri fizice). În ceea ce privește fenomenele naturale, este rareori suficient pentru a acoperi evenimente grave – deși acestea sunt rare. În general, astfel de servicii ar îmbunătăți doar situațiile de zi cu zi.

Calitatea serviciului evaluat ca fiind de nivelul 3

Serviciul este mai eficient și rezistă la atacurile și evenimentele descrise mai sus, dar ar putea fi insuficient împotriva atacurilor specializate (hackeri bine echipați și cu experiență, ingineri de sistem specializați, mai ales dacă aceștia au unelte sau expertiză aplicată pe domeniu, spioni profesioniști, și așa mai departe), sau dezastre naturale cu adevărat excepționale. O soluție generalizată ar avea un oarecare efect asupra unui număr mare de circumstanțe. Totuși, ea nu ar oferi cu siguranță nici o garanție pentru probleme sau atacuri foarte grave.

Calitatea serviciului evaluat ca fiind de nivelul 4

Acesta este cel mai ridicat nivel, și serviciul de securitate va rămâne activ și eficient în fața tuturor agresiunilor descrise mai sus. Ar putea totuși fi spart în circumstanțe excepționale: cei mai buni spărgători de coduri din lume cu cele mai bune unelte de spart coduri (ceea ce este posibil dacă unele țări vor ca acest lucru să se întâmple) sau o combinație excepțională de circumstanțe excepționale.

Procesul de evaluare a calității serviciului de securitate folosit de MEHARI a fost construit pentru a oferi evaluări de calitate corespunzătoare pentru definițiile de mai sus.

3.2 Evaluarea directă a calității serviciului de securitate

Folosind definițiile calității serviciului de mai sus, nivelul calității fiecărui serviciu poate fi evaluat direct.

„Manualul de referință al serviciului de securitate” oferit cu baza de cunoștințe, este o unealtă valoroasă pentru o astfel de evaluare. El conține descrieri ale fiecărui serviciu de securitate. Fiecare descriere acoperă:

- Obiectivele serviciului, și rezultatele așteptate.
- Mecanisme și soluții care ar putea sau ar trebui să fie folosite pentru a obține funcția necesară de la serviciu.
- Criterii care ar trebui luate în calcul la stabilirea calității serviciului. Aceste criterii se referă în mod explicit la eficiența, robustețea, și permanența serviciului.

3.3. Evaluarea calității serviciului de securitate folosind chestionare MEHARI

Pe lângă metoda în sine, metodologia MEHARI cuprinde baze de cunoștințe. Una din aceste baze de cunoștințe este o bază de audit a serviciilor de securitate pentru audit, compusă din chestionare și un sistem de evaluare pentru răspunsurile la întrebările din ele.

Chestionarele cuprind *un set de întrebări pentru care este necesar un răspuns de tipul da/nu*, cu un sistem asociat de notare și evaluare pe care îl vom examina mai târziu în acest document.

Mai jos este un extras din chestionar, care prezintă întrebări privind domeniul „arhitecturii sistemului”.

Întrebarea nr.	Chestionar de audit: Securitatea Arhitecturii sistemelor (07)
	Întrebare
A – Controlul accesului la sisteme și aplicații	

<i>A 02</i>	<i>Managementul autorizațiilor și privilegiilor de acces (oferire, delegare, revocare)</i>
07A02-01	Necesită procedura de acordare a autorizării accesului aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?
07A02-02	Autorizațiile sunt acordate către indivizii numiți doar ca o funcție a profilului lor?
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizației către o persoană (fie direct sau prin profilul său) strict controlată?
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizații la momentul plecării personalului sau la finalul contractului pentru personalul extern sau la schimbarea funcției?
07A02-05	Există un proces strict controlat (precum cel de sus) care permite delegarea autorizației proprii, în parte sau în întregime, unei persoane la alegere pentru o perioadă de timp determinată (în cazul absenței)?
07A02-06	Este posibil să se controleze în orice moment, pentru toți utilizatorii, drepturile, autorizațiile și privilegiile în vigoare?
07A02-07	Există un audit regulat, cel puțin o dată pe an, al profilurilor și autorizațiilor acordate tuturor utilizatorilor și al procedurilor pentru managementul profilurilor atribuite?

Chestionarele cuprind întrebări de diferite feluri. Acestea ar putea fi întrebări orientate către eficacitatea măsurilor de securitate (ex.: frecvență back-up-ului, tipul controlului accesului fizic: cititor de carduri, digicod, etc., existența detectoarelor de incendiu, etc.), întrebări orientate către robustețea măsurilor de securitate (ex.: unde sunt depozitate rezervele, și cum este protejat accesul, dacă există o ușă dublă, și cât de bine sunt construite ușile, cum este protejat sistemul de detectare a incendiilor, etc.). În general, sunt și una sau două întrebări despre monitorizarea, controlul și auditul funcțiilor așteptate de la serviciu.

3.3.1 Tipuri de chestionare

Bazele de cunoștințe MEHARI cuprind multe chestionare, fiecare specializat pe domenii, așa cum este descris în paragraful 2.2.1: Domenii de responsabilitate Mehari.

3.3.2 Sistemul de evaluare

Întrebările privind un serviciu de securitate depind de măsurile de securitate utile sau necesare ale aceluia serviciu. Totuși, nu toate măsurile au același rol de jucat, și trebuie făcută o distincție între măsuri contributive, măsuri majore sau suficiente, și măsuri esențiale.

3.3.2.1 Măsuri contributive

Anumite întrebări au legătură cu măsuri care au un anumit rol în contribuția la calitatea serviciului, fără ca implementarea lor totală să fie neapărat necesară.

În termeni cantitativi, o evaluare clasică aplicată la aceste măsuri reflectă ideea de contribuție. În acest caz, anumite măsuri – mai importante decât altele – ar avea o valoare diferită. Baza de cunoștințe MEHARI arată valoarea aplicată fiecărei întrebări.

Tabelul de mai jos mărește extrasul de mai devreme din baza de cunoștințe MEHARI. În el, o coloană este rezervată pentru răspunsurile la întrebări (1 pentru da, 0 pentru nu): coloana următoare arată valoarea aplicată răspunsurilor.

Întrebarea nr.	Chestionar de audit: Securitatea Arhitecturii sistemelor (07)		
	Întrebare	DA/NU	V

A – Controlul accesului la sisteme și aplicații			
A 02 Managementul autorizațiilor și privilegiilor de acces (oferire, delegare, revocare)			
07A02-01	Necesită procedura de acordare a autorizare a accesului aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?	0	4
07A02-02	Sunt acordate autorizațiile către indivizii numiți doar ca o funcție a profilului lor?	1	2
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizației către o persoană (fie direct sau prin profilul său) strict controlată?	1	4
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizații la momentul plecării personalului sau la finalul contractului pentru personalul extern sau schimbarea funcției?	0	2
07A02-05	Există un proces strict controlat (precum cel de sus) care permite delegarea autorizației propriie, în parte sau în întregime, unei persoane la alegere pentru o perioadă de timp determinată (în cazul absenței)?	0	4
07A02-06	Este posibil să se controleze în orice moment, pentru toți utilizatorii, drepturile, autorizațiile și privilegiile în vigoare?	1	1
07A02-07	Există un audit regulat, cel puțin o dată pe an, al profilurilor și autorizațiilor acordate tuturor utilizatorilor și al procedurilor pentru managementul profilurilor atribuite?	0	1

Valorarea medie evaluată este pur și simplu suma măsurilor active evaluate (cele ale căror răspuns este „da”), plus suma valorii posibile, rezultatul fiind normalizat pe o scară de la 0 la 4. Deci, dacă R_i este răspunsul la întrebarea i , W_i este valoarea lui i și M_w valoarea medie stabilită:

$$M_w = 4 * \sum R_i * W_i / \sum W_i$$

Deci, pentru răspunsurile arătate în chestionarul de exemplu de mai sus, valoarea medie stabilită este:

$$M_w = 4 * 7 / 18 = 1,6$$

Iar calitatea serviciului, $Q = M_w = 1,6$

3.3.2.2 Măsuri majore sau „suficiente”

Unele măsuri ar putea fi considerate suficiente pentru a asigura un anumit nivel de calitate al serviciului. De exemplu, un sistem de detectarea a incendiilor poate fi considerat suficient în oferirea nivelului 2 pentru sub-serviciul corespondent.

De aceea am adăugat un prag minim, care reprezintă nota minimă pentru calitatea serviciului dacă măsura este activă.

Coloana „Min” arată că dacă este dat un răspuns pozitiv la o întrebare pentru care a fost fixat un prag minim, atunci acel prag a fost atins sau întrecut de către sub-serviciu.

Mi jos este prezentată o lată privire asupra tabelului de mai devreme, de această dată cu coloana pentru min adăugată.

Întrebarea nr.	Chestionar de audit: Securitatea Arhitecturii sistemelor (07)			
	Întrebare	DA/NU	V	Min
A – Controlul accesului la sisteme și aplicații				
A 02 Managementul autorizațiilor și privilegiilor de acces (oferire, delegare, revocare)				
07A02-01	Necesită procedura de acordare a autorizare a accesului aprobarea	0	4	

	oficială a managementului de linie (la un nivel suficient de înalt)?			
07A02-02	Sunt acordate autorizațiile către indivizii numiți doar ca o funcție a profilului lor?	1	2	
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizației către o persoană (fie direct sau prin profilul său) strict controlată?	1	4	3
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizații la momentul plecării personalului sau la finalul contractului pentru personalul extern sau schimbarea funcției?	0	2	
07A02-05	Există un proces strict controlat (precum cel de sus) care permite delegarea autorizației propriie, în parte sau în întregime, unei persoane la alegere pentru o perioadă de timp determinată (în cazul absenței)?	0	4	
07A02-06	Este posibil să se controleze în orice moment, pentru toți utilizatorii, drepturile, autorizațiile și privilegiile în vigoare?	1	1	
07A02-07	Există un audit regulat, cel puțin o dată pe an, al profilurilor și autorizațiilor acordate tuturor utilizatorilor și al procedurilor pentru managementul profilurilor atribuite?	0	1	

În exemplu, faptul că procesul pentru alocarea, modificarea sau ridicarea drepturilor (întrebarea – 03) este administrat strict a fost considerat suficient pentru a mări nota calității serviciului la pragul de minim de 3.

3.3.2.3 Măsuri esențiale

Pe de altă parte, anumite măsuri pot fi considerate obligatorii în asigurarea unui anumit nivel al calității serviciului.

MEHARI asociază cu întrebările privind acele măsuri considerate obligatorii în asigurarea unui anumit nivel al calității, un prag al calității. Dacă pragul este depășit, implementarea măsurii este obligatorie.

Cu alte cuvinte, pragul arătat în coloana „Max” reprezintă nivelul maxim de calitate pe care sub-serviciul îl poate obține dacă măsura nu este implementată.

Atunci când există un conflict între pragul minim și cel maxim, valoarea maximă este cea care are prioritate.

Cu această adăugare la tabelul anterior obținem următoarea imagine:

Întrebarea nr.	Chestionar de audit: Securitatea Arhitecturii sistemelor (07)				
	Întrebare	DA/NU	V	Max	Min
A – Controlul accesului la sisteme și aplicații					
A 02 Managementul autorizațiilor și privilegiilor de acces (oferire, delegare, revocare)					
07A02-01	Necesită procedura de acordare a autorizare a accesului aprobarea oficială a managementului de linie (la un nivel suficient de înalt)?	0	4		
07A02-02	Sunt acordate autorizațiile către indivizii numiți doar ca o funcție a profilului lor?	1	2	2	
07A02-03	Este procedura de acordare (sau schimbare sau revocare) a autorizației către o persoană (fie direct sau prin profilul său) strict controlată?	1	4		3
07A02-04	Există un proces sistematic de actualizare a tabelului de autorizații la momentul plecării personalului sau la finalul contractului pentru personalul extern sau schimbarea funcției?	0	2	2	
07A02-05	Există un proces strict controlat (precum cel de sus) care permite delegarea autorizației propriie, în parte sau în întregime, unei persoane la alegere pentru o perioadă de timp determinată (în cazul absenței)?	0	4		
07A02-06	Este posibil să se controleze în orice moment, pentru toți utilizatorii, drepturile, autorizațiile și privilegiile în vigoare?	1	1		
07A02-07	Există un audit regulat, cel puțin o dată pe an, al profilurilor și autorizațiilor acordate tuturor utilizatorilor și al procedurilor pentru managementul profilurilor atribuite?	0	1	2	

În exemplul de mai sus, opinia experților susține că răspunsurile negative la întrebările 1 și 7 înseamnă că nivelul calității serviciului nu poate fi mai mare de 2. Această limită are prioritate în fața valorii nivelului 3 propusă mai devreme.

Acest sistem triplu de măsurare a calității serviciului evită riscul de a vedea că se dă un nivel al calității supraevaluat unei serii de măsuri ineficiente atunci când măsurile esențiale nu sunt active sau, dimpotrivă, o serie de măsuri greșit estimate sub-evaluează calitatea serviciului atunci când o măsură esențială este implementată. Această abordare este una din caracteristicile distinctive ale MEHARI, oferind o valoare reală pe baza expertizei persoanelor care întrețin bazele de cunoștințe.

3.3.2.4 Întrebări inaplicabile

Anumite întrebări pot fi considerate inaplicabile pentru anumite organizații. În acest caz, estimarea întrebărilor va fi forțată la zero.

Trebuie acordată atenție pentru a se asigura că o întrebare inaplicabilă rămâne așa, indiferent de evoluția planificată a sistemului IT și a serviciilor de securitate.

3.4. Procesul de audit

3.4.1 Procesul de revizie

Din cauză că chestionarele de audit ale serviciului de securitate sunt organizate pe domenii de responsabilitate, odată ce schema de audit este definită, ele pot fi copiate pentru a acoperi orice variații ale domeniilor care vor fi analizate. La întrebări ar trebui să răspundă persoana sau persoanele corespunzătoare care sunt cel mai bine calificate pentru acel domeniu. Aceeași abordare generală poate fi

folosită pentru evaluarea directă a calității serviciului de securitate.

Se poate ca, în timpul auditului, anumite sub-servicii să pară a nu fi aplicabile pentru organizația dată. Chestionarele corespondente pot fi atunci șterse.

A răspunde doar cu da sau nu la chestionare poate crea uneori dificultăți. Răspunsurile normale ar putea fi:

- „În general, DA, dar există excepții”
- „În teorie, DA, dar în practică, nu sunt sigur că se aplică peste tot”
- „DA, parțial (X%)”
- „DA, se desfășoară chiar acum”
- „DA, este planificat, dar încă nu s-a aplicat”
- Etc.

Sfatul nostru în asemenea circumstanțe este:

Notați-vă întotdeauna orice explicații care însoțesc răspunsurile, și păstrați-le. În chestionarele din hârtie care sunt folosite în timpul ședințelor de audit, ar trebui adăugată o coloană cu „comentarii” pentru astfel de explicații.

Deoarece sistemul de notare necesită un răspuns cu „da” sau „nu”, auditorul de securitate va trebui să ia o decizie. Ruta „sigură” ar fi să răspundă „nu” la toate întrebările unde există o îndoială (precum răspunsurile de mai sus). Indiferent de alegere, este important ca răspunsurile să nu influențeze necorespunzător deciziile care rezultă din audit. Mai ales, nu ar trebui să ascundă nici o imperfecțiune.

Ar trebui purtat în minte, totuși, faptul că ar putea demotiva personalul și să dăuneze credibilității auditului să introducă un răspuns „nu” în acele zone care sunt în mod clar corectate și se află sub control – mai ales dacă sunt minore.

O abordare rezonabilă pare a fi să se răspundă cu „da” de fiecare dată când procesul de corectare și reacția la lipsa măsurilor sau a implementării este sub control, și cu „nu” dacă nu este cazul.

Observați că, pentru ca aceste răspunsuri să fie acceptabile, auditul trebuie să treacă printr-o ședință față în față între auditor și persoana responsabilă cu domeniul care este auditat, iar chestionarele trebuiesc completate în timpul acelei ședințe. Chestionarele completate de către persoana care este auditată fără prezența auditorului pot masca complet realitatea și pot introduce erori grave în audit și în calitatea acestuia per total.

3.4.2 Notarea și corectarea notării

Pentru acele note obținute prin chestionare, odată completate, poate fi făcută o notare a serviciilor de securitate. Acest lucru va fi făcut folosind sistemul de evaluare din MEHARI, după cum s-a explicat mai devreme.

Sistemul de evaluare a fost proiectat și acordat de către experții CLUSIF. Totuși, este posibil să apară anumite imperfecțiuni pe plan local. El nu poate, efectiv, să ia în considerare fiecare caz local sau specific care poate fi întâlnit în timpul unui audit, și nici nu poate fi adaptat specific la fiecare organizație.

Auditorul ar trebui, deci, înainte de a trage concluziile și de a prezenta concluziile auditului, să verifice dacă notarea folosită pentru fiecare serviciu și sub-serviciu este corespunzătoare, prin referirea la definițiile nivelelor de calitate obținute.

Este, deci, obligatoriu ca auditorul să fie un profesionist cu experiență în securitate.

4 Produse livrabile

Rezultatele brute reprezintă fie chestionarele completate, cu comentariile adiacente după cum s-a descris mai devreme, fie evaluarea directă a calității serviciului de securitate.

În general, produsele livrabile sunt prezentate printr-un număr de grafice sintetice.

4.1 Graficul sintetic al serviciului de securitate

Recenzia finală a vulnerabilității este de obicei prezentată ca un grafic tip „diagramă păianjen”, cu mai multe dimensiuni

- Pe serviciu de securitate (arătând diferitele sub-servicii și notarea acestora),
- Pe domeniu de responsabilitate (arătând diferitele servicii care compun domeniul și notarea acestora, obținută prin notarea medie a sub-serviciilor lor componente),
- Global (arătând diferitele domenii și notarea acestora).

4.2 Graficul sintetic „tematic”

Anumite servicii de securitate, deși apar în diferite domenii de audit, sunt complementare în atingerea unui obiectiv de securitate global. De aceea, pentru a avea o idee generală asupra calității planurilor de rezervă, va trebui să combinați rezultatele planurilor de securitate pentru rețea și IT, planurile de continuitate, planurile de securitate electrică, și așa mai departe.

CLUSIF a definit 16 „teme” care reprezintă domenii de securitate majore care pot fi folosite pentru a construi grafice. Acești indicatori, pentru care calculele sunt disponibile în baza de cunoștințe MEHARI, sunt:

- Organizația de securitate (roluri și structuri),
- Conștientizarea și antrenarea în securitate,
- Securitatea locației fizice (controlul accesului, instalația),
- Controlul accesului în zonele sensibile,
- Protecția contra diferitelor riscuri (incendiu, inundații, etc),
- Securitatea arhitecturii rețelei (controlul accesului, sub-rețelele logice, firewall-urile, nivelele serviciului, etc),
- Confidențialitatea comunicațiilor și managementul integrității,
- Controlul accesului logic (sisteme, aplicații, și date),
- Securitatea datelor,
- Proceduri operaționale,
- Managementul mediului IT,
- Managementul crizei și planurile de rezervă,
- Rezervele, planificarea lor și planurile de restaurare a serviciului,
- Întreținerea,
- Securitatea proiectului IT și a dezvoltării,
- Managementul incident.

Merită observat faptul că, în timpul unui audit parțial, prin acoperirea uneia sau a mai multor teme (de exemplu întreținerea, sau securitatea proiectelor de dezvoltare) este mai ușor să concentrăm auditul asupra serviciilor de securitate care contribuie la temele selectate.

4.3 Măsuri de concordanță legate de standardul ISO 17799:2005

După cum s-a explicat în documentul MEHARI „*Concepte generale și mecanisme principale*”, o recenzie Ghid de evaluare pentru serviciile de securitate

a securității poate servi la fel de bine ca mijloc de a documenta nivelul de bună practică recomandat de către standardul ISO 17799:2005.

Efectiv, fiecare întrebare din procesul de audit MEHARI poate fi văzută ca un punct de control elementar care este menit să valideze soluții și procese de securitate implementate de entitatea organizațională.

Deoarece organizarea auditului MEHARI aduce la lumină capacitatea de a reduce riscul, la fiecare nivel operațional și cu contribuția managerilor operaționali, structura serviciilor nu este perfect aliniată cu structura „descriptivă” a standardului.

În plus, chestionarele MEHARI conțin mai multe servicii și controale care merg mai departe de recomandările standardului. De aceea a fost făcută o aplicație a întrebărilor MEHARI pe practicile standardului ISO.

Chestionarele de audit MEHARI 2007 au fost puțin modificate pentru a facilita această aplicație și se oferă oferit un tabel al corespondențelor (cu formulele corespunzătoare) în baza de date a cunoștințelor.

Astfel este posibil să se vizualizeze¹ nivelul de maturitate al entității operaționale pentru fiecare punct de control al standardului (cu o notare de la 0 la 4, de exemplu). Acesta nu reprezintă scopul primar al lui MEHARI, dar poate oferi informații utile în timpul procesului de certificare sau atunci când se compară diferite organizații.

¹ Instrumentul RISICARE oferă acest nivel de vizualizare
Ghid de evaluare pentru serviciile de securitate

5 Sfaturi practice

5.1. Puncte importante care trebuie incluse în schemele de audit

O schemă de audit este percepută uneori ca fiind complicată. Nu există nici un motiv pentru acest lucru – ea este doar o fotografie a stării a diferite soluții și situații.

Un sistem mainframe este diferit de unul UNIX; iar sistemele lor de securitate, precum și operațiunile lor, sunt inevitabil diferite. Aceste diferențe pot fi ignorate sau luate în calcul, în funcție de circumstanțe. Dacă se vrea ca diferențele să fie scoase la iveală, chestionarele ar trebui multiplicat corespunzător, și ar trebui puse întrebări asemănătoare unor grupuri diferite. Dacă preferați să ignorați diferențele, întrebările vor fi puse doar o dată la nivel global – ***dar acest lucru este independent de metodologia auditului.***

Schema de audit este doar un mijloc simplu de a diferenția diferitele domenii ale soluției în timpul procesului de audit.

Distincția dintre domeniile soluției este doar o chestiune de alegere. O abordare de obicei bună pentru această problemă este să se ia în considerare câte persoane vor trebui interviuate pentru același domeniu.

Practic, întrebarea este „***câte persoane diferite pot avea atât de multe păreri diferite asupra aceleiași situații?***”. Deoarece fiecare părere diferită necesită un interviu specific, iar două păreri foarte asemănătoare pot să nu justifice timpul și energia interviurilor separate.

5.2 Puncte importante care trebuie acoperite în procesul de audit

Am insistat deja asupra necesității ca chestionarele să fie completate în timpul interviurilor față în față, așa că acele comentarii și așa mai departe pot fi și ele incluse.

De asemenea am sugerat, acolo unde răspunsurilor nu sunt în mod clar „da” sau „nu”, că este mai bine să se ia o abordare pesimistă, în timp ce se adaugă explicațiile ca și comentarii, arătând o parte mai pozitivă.

Bazele de cunoștințe MEHARI, și, mai ales chestionarele pentru audit, au fost concepute folosind următorul principiu de avertizare:

Procedurile automate ale abordării nu trebuie să permită niciodată unui risc să fie subevaluat. Este întotdeauna preferabil ca un risc să fie supraevaluat inițial, atunci când poate fi redus mai târziu, decât să fie subevaluat și să nu apară într-o analiză mai detaliată.

Unul din principiile de bază este să se încerce evitarea cazurilor în care procedurile automate ar elimina un scenariu ca fiind un risc scăzut, când acesta ar putea fi foarte grav. La subevaluarea gravității unui scenariu contribuie mai mulți factori, dintre care, supraevaluarea anumitor servicii de securitate.

Urmând acest principiu, de vreme ce rezultatele unui audit de securitate ar putea fi folosite pentru a analiza riscurile întâlnite de o organizație în general, notarea aplicată serviciilor de securitate este destul de prudentă.

Notarea finală poate părea severă uneori, atunci când este comparată cu ale sisteme de audit. Cititorul ar trebui să rețină faptul că MEHARI insistă că serviciile de securitate trebuie să fie eficiente, robuste și permanente, ceea ce înseamnă că sunt supuse unui control regulat. Cuvântul nostru final este că noi căutăm să oferim asigurarea securității prin această abordare. Acesta nu este întotdeauna cazul cu alte abordări.