MEHARI 2007

Ghid de analiză a riscului

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

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

O recenzie a principiilor analizei riscurilor şi identificarea situațiilor de risc este dată în documentul „*MEHARI - Concepte şi Mecanisme*”. Principalele puncte sunt amintite mai jos:

- O situație de risc poate fi caracterizată prin potențialitatea şi impactul său intrinsec, în absența oricăror măsuri de securitate.
- Potențialitatea intrinsecă şi impactul intrinsec pot fi evaluate.
- Măsurile de securitate pot fi aplicate pentru a reduce riscul prin factori semnificativi de reducere a riscului.

Analiza unei situații de risc poate fi făcută direct folosind principiile generale şi explicațiile oferite în documentul „*MEHARI - Concepte şi Mecanisme*”.

Dacă situația de risc care este analizată corespunde unuia din scenariile cuprinse în baza de cunoştințe MEHARI, este posibil şi - pentru o evaluare directă a nivelului riscului – să se utilizeze „*Manualul de referințe pentru scenarii de risc*”. Documentul oferă, pentru fiecare scenariu, indicații specifice despre factorii de reducere a riscului.

În acest document descriem modul în care procedurile automate MEHARI ar trebui folosite pentru a ajuta la evaluarea unei situații de risc. Exemplele care sunt folosite vor fi cele în care situația care este analizată corespunde unui scenariu din baza de cunoştințe MEHARI.

De asemenea vom descrie modul în care trebuie folosite procedurile automate pentru a evidenția situațiile de risc şi pentru a le selecta pentru o analiză detaliată.

2 Analiza situațiilor de risc

2.1 Trecerea în revistă a procesului de analiză a riscului

Figura 1, de mai jos, arată procesul total pentru analiza riscului, după cum a fost deja descris în documentul „*MEHARI – Concepte şi mecanisme*”.

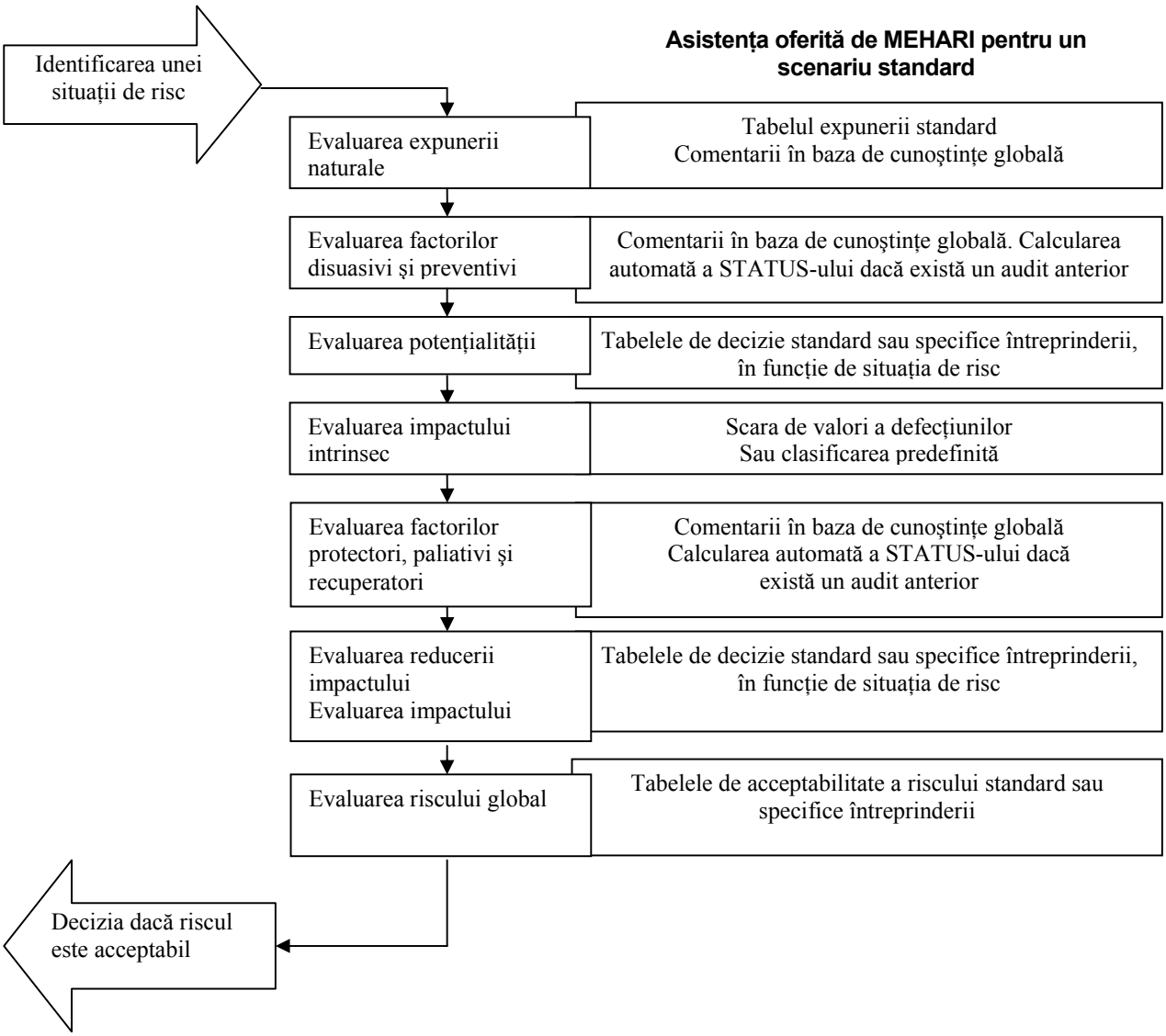


Figura 1: Procesul de analiză a riscului şi asistența oferită de MEHARI

Astfel, prin baza sa de cunoştințe, MEHARI propune diferite ajutoare pentru analiza riscului.

- Asistență în evaluarea expunerii naturale
- Proceduri automate pentru evaluarea factorilor de reducere a riscului (factori disuasivi, preventivi, protectori, paliativi şi recuperatori) în funcție de calitate serviciilor de securitate,

dacă acestea au fost evaluate prin un audit MEHARI.

- Un tabel generic al impactului intrinsec poate fi creat ca rezultat al clasificării sau direct folosind o scară a valorilor defecțiunilor.
- Proceduri automate pentru calcularea potențialității şi impactului actual, ca funcție a factorilor expunerii naturale, impactului intrinsec, şi de atenuare a riscului.

Toate aceste ajutoare sunt disponibile automat pentru toate scenariile din baza de cunoştințe MEHARI.

2.2 Evaluarea expunerii naturale

Am explicat deja, în documentul „MEHARI - Concepte şi Mecanisme", că expunerea naturală poate varia pentru aceeaşi organizație în funcție de fenomene conjuncturale.

Totuşi, pentru multe organizații, rămâne adevărat faptul că expunerea „normală" sau „standard" la un anumit tip de risc (de ex. în absența oricărui fenomen excepțional anume) este în conformitate cu ceea ce poate fi observat în general, şi poate fi făcută o evaluarea în prealabil.

2.2.1.Expunerea naturală standard

Scenariile[1] din baza de cunoştințe MEHARI sunt comparate cu o listă de evenimente caracteristice, fie că sunt accidente, erori sau acțiuni voluntare (malițioase sau nu), şi pentru care este propusă o evaluare „standard" anterioară a expunerii.

Deci, de exemplu, este estimat că expunerea naturală „standard" la incendii pentru o întreprindere este de nivel 2 (destul de improbabil); la pierderea unui serviciu al echipamentului ICT este de nivel 3 (destul de probabil); iar la o eroare în timpul procesului de introducere a datelor este de nivel 4 (foarte probabil).

Lista acestor evenimente şi a expunerii naturale standard este dată în Anexa 1.

Fiecare scenariu se referă la un tip de eveniment, după cum este arătat în exemplul de mai jos:

10.31: Pierderea fişierelor de date, prin ştergerea răuvoitoare a mediilor de către personalul de operațiuni.

TYP-EXPO	EFF-DISS	EFF-PREV
MA010	MAX(MIN(07C02;08E02);08C01)	08A02
EFF-PROT	EFF-PALL	EFF-RECUP
MAX(08C01 ;08C05)	MAX(MIN(08D05;09D03);09D02)	01D02

Tipul de expunere MAO 10 din tabel în Anexa 1 este: „Ştergerea voluntară a datelor sau furtul de medii" şi este evaluat cu o valoare standard de nivel 3 (destul de probabil).

[1] Scenariile din baza de cunoştințe MEHARI sunt grupate pe familii care au consecințe similare.
În această versiune, există 12 familii standard de scenarii.

2.2.2 Expunerea naturală specifică întreprinderilor pentru un risc dat

Ar trebui făcut clar faptul că evaluarea standard oferită este doar o evaluare prin lipsă, şi că evaluarea specifică a expunerii întreprinderii la situația de risc analizată este cu mult mai preferabilă. Pentru o astfel de evaluare, faceți referire la definițiile nivelurilor de expunere date în documentul „MEHARI - Concepte şi Mecanisme". Acestea sunt rezumate în Anexa 2.

Pentru un scenariu specific, ar trebui de asemenea să consultați „Manualul de Referință al Scenariilor de Risc", care conține informații specifice despre evaluarea expunerii naturale.

NOTĂ:

Dacă situațiile de risc vor fi analizate sistematic, sau dacă mai multe situații de risc vor fi examinate, este preferabil să se înceapă cu trecerea în revistă a tuturor evenimentelor, şi să se facă o apreciere generală referitor la expunerea întreprinderii la fiecare dintre acestea.

2.3 Evaluarea impactului intrinsec

Definiția impactului intrinsec al unui scenariu, dată în „MEHARI – Concepte şi mecanisme", este evaluarea consecințelor evenimentului de risc care are loc efectiv, independent de orice măsuri de securitate.

Pentru fiecare din scenariile definite în baza de cunoştințe MEHARI, există o țintă a scenariului (un bun care va fi deteriorat sau afectat de scenariu).

Aceasta ar putea fi un tip de date sau de informații care este furat, un tip de bunuri a cărui disponibilitate este redusă, sau un bun care este modificat. Acest lucru va depinde de faptul dacă scenariul va afecta confidențialitatea, disponibilitatea, sau integritatea bunului. Acestea sunt cele trei criterii de bază pe care MEHARI le acoperă ca standard.

Evaluarea impactului intrinsec în astfel de condiții implică evaluarea criticalității sau a gravității pierderii disponibilității, integrității sau confidențialității, în funcție de tipul de scenariu, şi de tipul de bunuri implicat în scenariu.

Abordarea clasificării folosită de MEHARI permite crearea unui tabel al clasificării generice. Acest tabel arată tipurile de bunuri identificate în mod specific prin scenariile din baza de cunoştințe. Abordarea clasificării este descrisă în documentului „*MEHARI – Concepte şi mecanisme*", şi în „*Analiza mizelor de securitate şi ghidul de clasificări*".

2.3.1 Tabelul impactului intrinsec

Abordarea folosită pentru a evalua impactul intrinsec poate fi apoi organizată. Constă în completarea unui tabel al impactului intrinsec, pe baza tabelului oferit în Anexa 3, din care este arătat un extras mai jos.

Tabelul impactului intrinsec			
Clasificarea datelor, informațiilor şi elementelor de infrastructură	A	I	C
Date şi informații			
D01 Dosare cu date, sau baze de date cu aplicații			
D07 Poştă şi faxuri			
.../...			
Infrastructura IT şi telecom			
R02 Echipament şi legături pentru rețeaua locală			
S01 Mainframe-uri, servere de aplicații			

Acest tabel este completat prin transcrierea nivelului de consecință sau de impact asupra disponibilității, integrității sau confidențialității pentru fiecare tip de bun identificat. Totuşi, anumite intrări nu vor fi completate, de exemplu cea pentru confidențialitatea unei componente hardware.

Abordarea de bază foloseşte tabelele de clasificare, după cum este descris în „*MEHARI Analiza mizelor de securitate şi ghidul de clasificare*".

În cel mai rău caz, poate fi făcută în mod direct, dar abordarea clasificării definită în „*MEHARI Concepte şi mecanisme*", aşa cum este completată de procesul de mai sus, este fără îndoială mai bună.

Principiul general pentru completarea tabelului impactului intrinsec este că se copie cea mai mare valoare a clasificării găsită în timpul procesului de clasificare pentru fiecare tip de informație şi pentru fiecare criteriu. Detaliile despre modul de completare al tabelului impactului intrinsec din rezultatele clasificării sunt descrise în „*MEHARI Analiza mizelor de securitate şi ghidul de clasificare*".

Acest lucru produce deci o sinteză care poate fi folosită pentru a defini nivelul impactului intrinsec pentru fiecare din scenariile din baza de cunoştințe MEHARI care au impact asupra tipului de informații sau de bunuri de la fiecare examinare.

2.3.2 Extinderea tabelului impactului intrinsec

Tabelul MEHARI standard se referă doar la trei criterii standard: disponibilitate, integritate şi confidențialitate. Alte criterii pot, desigur, să fie folosite. Tabelul poate fi extins pentru a include criterii precum, dovadă, capacitatea de a fi urmărit, capacitatea de a fi auditat, şi aşa mai departe.

Pentru a efectua o astfel de extindere, ar trebui create scenarii care aduc noile criterii în joc (sau modifică scenariile existente). În plus, tabelele de evaluare corespondente ar trebui definite.

Pachetul software Risicare[2] permite să fie luate în considerare până la opt criterii.

[2] Marcă înregistrată a BUC S.A.

2.3.3 Evaluarea scenariilor impactului intrinsec

Impactul intrinsec al fiecărui scenariu al bazei de cunoştinţe este evaluat destul de simplu. Fiecare scenariu are o legătură cu un tip de bunuri în tabelul impactului intrinsec şi un criteriu de aplicare (A, I sau C – sau, poate, altele).

Altfel spus, fiecare scenariu din baza de cunoştinţe face referire în mod explicit la un tip de bunuri afectat de scenariu, şi la modul în care este afectat (A, I sau C). În acest mod, impactul intrinsec poate fi evaluat folosind tabelul din Anexa 3.

2.3.4 Descompunerea cartografică

Tabelul standard al impactului intrinsec, aşa cum este dat în Anexa 3, arată doar o singură linie pentru toate serverele de aplicaţii sau mainframe-urile. De asemenea, există o singură linie pentru toate bazele de date cu aplicaţii – şi în general doar o singură referinţă pentru fiecare tip de bunuri.

Această abordare globală permite analiza situaţiilor de risc luând în considerare sensibilitatea maximă a bunurilor în discuţie, fără a diferenţia între bunuri, sau a le numi. Aceasta este o simplificare care restricţionează situaţiile care pot fi analizate, fără consecinţe practice, deoarece va exista întotdeauna o oportunitate, atunci când se construiesc planurile de acţiune, pentru a limita acţiunile corective pentru acele bunuri care sunt cele mai sensibile.

Totuşi, se poate distinge între diferite variaţii ale tipurilor de bunuri, tot aşa cum variaţiile serviciilor de securitate pot fi diferenţiate în timpul unui audit MEHARI. Pentru mai multe detalii, vezi schema de audit în „Ghidul de audit al serviciilor de securitate”.

Crearea variaţiilor a tipurilor de bunuri în tabelul impactului intrinsec este cunoscută ca **descompunere cartografică**. Aceasta permite diferenţierea, de exemplu, între servere în mai multe domenii diferite, domenii de baze de date de aplicaţii, a software-ului în domenii, şi aşa mai departe. Utilizarea descompunerii cartografice permite tratamentul specific al unuia sau a mai multor domenii specifice de activitate.

Pachetul software Risicare™ foloseşte posibilitatea de a crea variaţii de scenarii în funcţie de variaţiile cartografice care sunt create[3].

ATENŢIE: Utilizarea acestei opţiuni poate, totuşi, complica mult sarcina, deoarece va crea în mod inevitabil mai multe scenarii.

2.4 Evaluarea factorilor de reducere a riscului printr-un audit de securitate MEHARI

Evaluarea potenţialităţii impactului unui scenariu de risc depinde de analiza existenţei factorilor de

[3] Atunci când Risicare nu este folosit pentru această lucrare, şi când foile de calcul din Excel ale bazei de cunoştinţe standard a Clusif sunt folosite, tabelul de clasificări T1 descris în documentul „Mehari Principii de bază şi Concepte generale” ar trebui modificat. Tabelul impactului intrinsec oferit în Anexa 3 ar trebui de asemenea modificat pentru a lua în considerare descompunerea cartografică.

reducere a riscului, şi de o evaluare a nivelurilor acestora.

Factorii de reducere a riscului sunt disuasiunea şi prevenția pentru potențialitate, protecție, paliativ şi recuperare pentru impact.

În baza sa de cunoştințe, MEHARI oferă evaluări ale nivelurilor acestor factori de reducere a riscului, în funcție de calitatea serviciilor de securitate potrivite pentru scenariul care este analizat.

Această evaluare automată este efectuată în doi paşi:

- Calcularea indicatorilor de eficacitate pentru serviciile de securitate, pentru fiecare tip de factor de reducere a riscului,
- Calcularea factorilor de reducere a riscului înşişi.

2.4.1 Indicatorii de eficacitate pentru serviciile de securitate pe scenariu şi măsura reducerii riscului

MEHARI defineşte un indicator de eficacitate pentru fiecare scenariu şi pentru fiecare tip de măsură de reducere a riscului.

Eficacitatea pentru fiecare măsură de reducere a riscului este arătată cu următoarele notări:

EFF-DISS pentru eficacitatea *măsurilor disuasive*
EFF-PREV pentru eficacitatea *măsurilor preventive*
EFF-PROT pentru eficacitatea *măsurilor protectoare*
EFF-PALL pentru eficacitatea *măsurilor paliative*
EFF-RECUP pentru eficacitatea *măsurilor recuperatoare*

Aceşti indicatori sunt calculați folosind formule care fac toată diferența pentru serviciile de securitate.

Formulele oferite în baza de cunoştințe MEHARI apelează la:

- Fie la un serviciu de securitate direct, prin identificatorul[4] său, atunci când serviciul este singurul care are acest tip de efect asupra scenariului;
- Sau formule care conțin funcții: MIN (arg1; arg2; ...) sau MAX (arg1; arg2; ...), parametrii (arg1; arg2; ...) fiind identificatori ai serviciilor de securitate ai bazei de cunoştințe MEHARI.

Formulele pot deci să aibă următoarele forme, de exemplu:

EFF-PALL = 06B01
EFF-PREV = MAX(04B04;MIN(04B01;04B02;04B03))

Prima formulă semnifică faptul că eficacitatea (propusă) a măsurilor paliative este o funcție directă a serviciului 06B01 şi ia ca valoare nivelul de calitate a acelui serviciu.

A doua formulă semnifică faptul că eficacitatea (propusă) a măsurilor preventive este egală cu valoarea mai mare dintre calitatea serviciului a 04B04 şi funcția care reprezintă minimul serviciilor 04B01, 04B02, şi 04B03.

[4] Identificatorul unui sub-serviciu este compus dintr-un număr de domeniu, o literă care indică serviciul la care este ataşat, şi un număr de sub-serviciu (ex.: 06B01)

NOTĂ:

Funcția MIN înseamnă că serviciile numite ca parametri sunt complementare. Dacă nivelul unuia este mic, nivelul întregului va fi mic. Un exemplu al unui astfel de caz se găseşte în managementul accesului utilizatorului şi autentificarea; dacă unul din ele are un nivel mic, întregul control al accesului se află la un nivel mic.

Funcția MAX semnifică că serviciile numite parametri sunt alternative. Dacă unul din servicii are un nivel al calității ridicat, atunci întregul va avea un nivel al calității ridicat. Un exemplu pentru un astfel de caz, în funcție de anumite scenarii, îl reprezintă controlul accesului la date şi criptarea datelor.

Este posibil ca nici unul din serviciile de securitate existente să nu aibă o influență asupra unui tip de reducere a riscului dat pentru un scenariu dat.

Ca un exemplu, ilustrația de mai jos arată conținutul bazei de cunoştințe MEHARI pentru scenariul 10.31:

10.31: Pierderea fişierelor de date, prin ştergerea răuvoitoare a mediilor de către personalul de operațiuni.

TYP-EXPO	EFF-DISS	EFF-PREV
MA010	MAX(MIN(07C02; 08E02);08C01)	08A02
EFF-PROT	EFF-PALL	EFF-RECUP
MAX(08C01;08C05)	MAX(MIN(08D05;09D03);09D02)	01D02

2.4.2 Factorii de reducere a riscului „calculat”

În mod clar, coeficienții de eficacitate evaluați mai sus (EFF-XXXX) sunt calculați pe baza valorilor calității serviciului, care nu au de ce să fie valori întregi, şi coeficienții de eficacitate nu sunt nici ei înşişi valori întregi. Pentru a face evaluarea finală a potențialității şi a impactului mai uşoară, MEHARI le transformă în valori întregi pentru evaluarea factorilor de reducere a riscului.

În MEHARI, factorii de reducere a riscului sunt notați cu STATUS-XXXX (de exemplu STATUS-DISS pentru factorul de disuasiune).

Valorile pentru STATUS sunt obținute prin rotunjirea valorii la cel mai apropiat număr întreg:
STATUS-XXXX = 1 dacă EFF-XXXX< 1,5 STATUS-XXXX = 2 dacă 1,5 < EFF-XXXX < 2,5
STATUS-XXXX = 3dacă 2,5 < EFF-XXXX < 3,5 STATUS-XXXX = 4 dacă 3,5 < EFF-XXXX
Unde XXXX poate fi DISS, PREV, PROT, PALL sau RECUP

Notă:
Valoarea pentru evaluarea expunerii naturale va fi de asemenea dată prin notarea STATUS-EXPO.

Aceşti factori de reducere a riscului sunt factorii „calculați”. Asta înseamnă că valoarea obținută poate să nu fie în totalitate pertinentă în contextul specific al întreprinderii sau organizației. Este

posibil să existe situații, de exemplu, când personalul nu este sensibil la măsurile disuasive, când personalul este format din experți, unde măsurile preventive nu au însemnătate, şi situații unde măsurile de protejare sau paliative nu ar avea nici un efect asupra impactului real.

MEHARI ajută prin oferirea de valori calculate pentru factorii de reducere a riscului. Aceste valori ar trebui, totuşi, să fie verificate înainte de a le aplica.

Un caz deosebit de frecvent este cel al scenariilor pentru care se poate considera că măsurile protectoare nu ar reduce semnificativ impactul intrinsec al scenariului (deoarece detectarea fraudei sau dezvăluirea informațiilor, de exemplu, nu ar reduce gravitatea riscului, indiferent de măsurile aplicate). Un astfel de scenariu poate fi considerat non-evolutiv, şi poate fi declarat ca atare[5].

2.4.3 Evaluarea factorilor de risc

Factorii de risc pentru un scenariu dat ar trebui verificați contra definițiilor lor de bază înainte de a-i aplica la scenariu, (vezi Anexa 4).

2.5. Evaluarea potențialității şi a impactului

2.5.1 Evaluarea automată a potențialității: STAUS-P

MEHARI oferă o evaluare automată a potențialității, începând cu o evaluare a expunerii naturale (STATUS-EXPO), pe de o parte, şi nivelurile măsurilor disuasive şi preventive (STATUS-DISS şi STATUS-PREV), pe de altă parte.

Din expresia STATUS-ului de mai sus în numere întregi, MEHARI evaluează potențialitatea sub denumirea STATUS-P. Aceasta este dedusă direct din STATUS-EXPO, STATUS-DISS şi STATUS-PREV de tabelele de evaluare.

În MEHARI sunt folosite trei tabele standard, în funcție de motivele pentru accidentul sau evenimentele care conduc la scenariu:

- Eveniment natural sau accident
- Eroare umană
- Acțiune umană voluntară (malițioasă sau nu).

Aceste tabele standard pot fi modificate dacă este necesar.

Notă:

Logica din spatele acestor tabele de evaluare este să se considere că pentru fiecare tip de cauză (accident, eroare sau acțiune voluntară), ar trebui urmat acelaşi raționament independent de descrierea precisă a scenariului. Cu niveluri de expunere, disuasiune, şi prevenție egale, potențialitatea a două scenarii ar trebui să fie aceeaşi.

[5] În Risicare, această opțiune este disponibilă pentru scenarii care sunt inițial considerate evolutive. Selectarea acestei opțiuni are efectul de a forța aplicarea unui anumit tabel de evaluare care nu ia în considerare măsurile protectoare.

2.5.2 Evaluarea automată a impactului: STATUS-I

MEHARI oferă şi o evaluare automată a impactului, pornind de la impactul intrinsec al scenariului pe de o parte şi nivelurile de măsuri protectoare, paliative şi recuperatoare (măsurate de STATUS-PROT, STATUS-PALL şi STATUS-RECUP), pe cealaltă parte.

Evaluarea este formată din doi paşi:

- Evaluarea unui indicator de reducere a impactului: STATUS-RI
- Evaluarea impactului: STATUS-I

2.5.2.1 Evaluarea reducerii impactului: STATUS-RI

MEHARI oferă inițial o evaluare a reducerii impactului, reprezentată de indicatorului STATUS-RI. Aceasta este dedusă direct din STATUS-PROT, STATUS-PALL şi STATUS-RECUP prin tabele de evaluare. Acest factor de reducere a impactului măsoară atenuarea consecințelor riscului, în comparație cu impactul intrinsec evaluat în prealabil.

MEHARI foloseşte trei tabele standard de evaluare pentru a evalua STATUS-RI, în funcție de tipul de consecință al scenariului:

- Pierderea disponibilității
- Pierderea integrității
- Pierderea confidențialității

Aceste tabele iau în considerare şi dacă scenariul este evolutiv sau nu. Această caracteristică este definită explicit în baza de cunoştințe. Ea poate fi forțată la un status non-evolutiv pentru acele scenarii care au fost inițial declarate în bază ca fiind evolutive.

Aceste tabele standard pot fi şi modificate dacă este necesar.

Notă:

Logica din spatele acestor tabele de evaluare este să se considere că pentru fiecare tip de consecință (pierderea, disponibilității, integrității sau confidențialității), ar trebui urmat acelaşi raționament independent de descrierea precisă a scenariului. Cu niveluri egale de măsuri protectoare, paliative şi recuperatoare, reducerea impactului intrinsec pentru două scenarii comparabile ar trebui să fie aceeaşi.

2.5.2.2 Evaluarea impactului: STATUS-I

Impactul rezidual este dedus din impactul intrinsec şi indicatorul de reducere a impactului prin următoarea formulă:

I = MIN (INTRINSIC IMPACT; 5 - STATUS-RI)

Ceea ce înseamnă că STATUS-RI are efectul de a defini nivelul maxim al impactului:

- Nivelul maxim de impact 4 dacă STATUS-RI este 1
- Nivelul maxim de impact 3 dacă STATUS-RI este 2

- Nivelul maxim de impact 2 dacă STATUS-RI este 3
- Nivelul maxim de impact 1 dacă STATUS-RI este 4

Evaluarea STATUS-I poate fi reprezentată şi prin tabelul de mai jos:

Tabelul de calcul pentru STATUS-I				
STATUS-RI → Impact intrinsec ↓	1	2	3	4
4	4	3	2	1
3	3	3	2	1
2	2	2	2	1
1	1	1	1	1

2.5.3 Principii de construire a tabelului de evaluare

În practică, tabelele standard, fie că sunt pentru potențialitate sau impact, sunt construite folosind un anumit număr de principii (descrise în Anexa 5 – Principii pentru construirea tabelelor de evaluare STATUS). Pentru a modifica aceste tabele, trebuie să se înceapă cu principiile, şi să se modifice după cum este necesar, apoi să se reconstruiască tabelele ca rezultat.

Tabelele de evaluare standard sunt documentate în Anexa 6.

2.5.4 Evaluarea potențialității şi a impactului

Precum şi pentru factorii de reducere a riscului, procedurile automate oferite prin tabelele de decizie oferă doar un ajutor în judecarea valorilor indicatorilor numiți *STATUS* în MEHARI.

O judecată finală ar trebui făcută, ca regulă generală, asupra pertinenței nivelurilor potențialității P şi ale impactului I.

2.6 Evaluarea gravității unui scenariu

Gravitatea unui scenariu va fi dedusă din evaluarea potențialității şi a impactului (P şi I), prin tabelul acceptabilității riscului, aşa cum este definit în documentul „*MEHARI – Concepte şi Mecanisme*”.

2.7 Exprimarea cerințelor de securitate

Acest pas este folosit doar atunci când se foloseşte managementul riscului la nivelul entității. Constă în evaluarea cerințelor consolidate, după evaluarea gravității tuturor situațiilor de risc identificate în timpul unui audit al serviciilor de securitate.

Această abordare este bazată pe definiția „**cerințelor de securitate**”, aşa cum este detaliată în Anexa 7.

2.8 Sfaturi practice

2.8.1 Gândirea din spatele abordării analizei riscului

Am arătat în mod intenționat modul în care procedurile automate ale MEHARI pot fi folosite în evaluarea nivelurilor de risc.

Este important să se rețină că acesta este un proces de evaluare, şi că consensul unui comitet de evaluare este întotdeauna mai de încredere decât procedurile automate.

2.8.2 Structura unui comitet de evaluare a riscului

Abordarea pe care am descris-o funcționează şi mai bine atunci când un grup sau comitet de lucru reprezentativ efectuează evaluarea riscului. Structura acestui comitet este deosebit de importantă, şi ar trebui să conțină:

- Utilizatori din zona în cauză. Aceştia ar trebui să aibă un profil care le permite să judece dacă măsurile de securitate vor aduce cu adevărat atenuarea necesară a consecințelor.
- Personal IT care poate să explice, celorlalți membri ai comitetului, eficacitatea diferitelor măsuri de securitate şi modul în care aceste măsuri ar putea fi împiedicate sau trecute (robustețea şi controlul/monitorizarea).
- Un facilitator care este bine versat în metoda însăşi, şi care are competențe specifice în securitatea IT.

2.8.3 Utilizarea abordării în conjuncție cu un audit de securitate

Am spus deja că procedurile automate ar trebui luate în considerare doar ca un ajutor în procesul de evaluare. Totuşi, este de asemenea posibil ca, chiar şi cu un comitet competent şi reprezentativ, calitatea serviciilor de securitate să fie supra-evaluată – fie prin optimism involuntar sau prin voință politică.

Un audit de securitate poate asigura în plus calitatea totală a abordării, şi poate oferi un punct de referință pentru a scoate la iveală şi alte întrebări.

Evaluarea riscurilor mari folosind procedurile automate poate scoate în evidență slăbiciuni sau vulnerabilități care ar fi trecut neobservate într-o evaluare directă. Orice diferență între aceste două abordări necesită examinare mai amănunțită.

În acest sens, confirmarea evaluării directe prin utilizarea procedurilor automate ar trebui considerată ca fiind o cea mai bună practică.

3 Identificarea situațiilor de risc

În capitolul anterior, am discutat despre analiza unui anumit isc.

Identificarea situațiilor care vor fi analizate reprezintă deci un pas preliminar pentru a stabili şi care unelte sunt necesare.

Există două metode principale de identificare a riscurilor:

- abordare directă, folosind scara valorilor defecțiunilor („*MEHARI – Concepte şi mecanisme*”).
- identificare organizată şi sistematică folosind o evaluare automată a bazei de scenarii oferită de MEHARI.

Această secțiunea va examina cea de-a doua din aceste opțiuni.

3.1 Identificarea sistematică folosind baza de cunoştințe

Vom acoperi aici asistența adusă se MEHARI în identificarea sistematică a situațiilor de risc.

Identificarea sistematică va folosi baza de cunoştințe a scenariilor de risc care a fost deja descrisă şi, mai ales, procedurile automate descrise în secțiunea anterioară. Este bazată pe o analiză preliminară care rezultă într-o scară de valori a defecțiunilor, o clasificare a bunurilor sistemului informațional şi un audit de securitate.

Procesul folosit de MEHARI este bazat pe o selecția unui set de scenarii care sunt specifice organizației care este studiată; întreaga întreprindere, o unitate operațională, etc.

Există doi paşi principali în proces, după cum se vede în figura de mai jos:

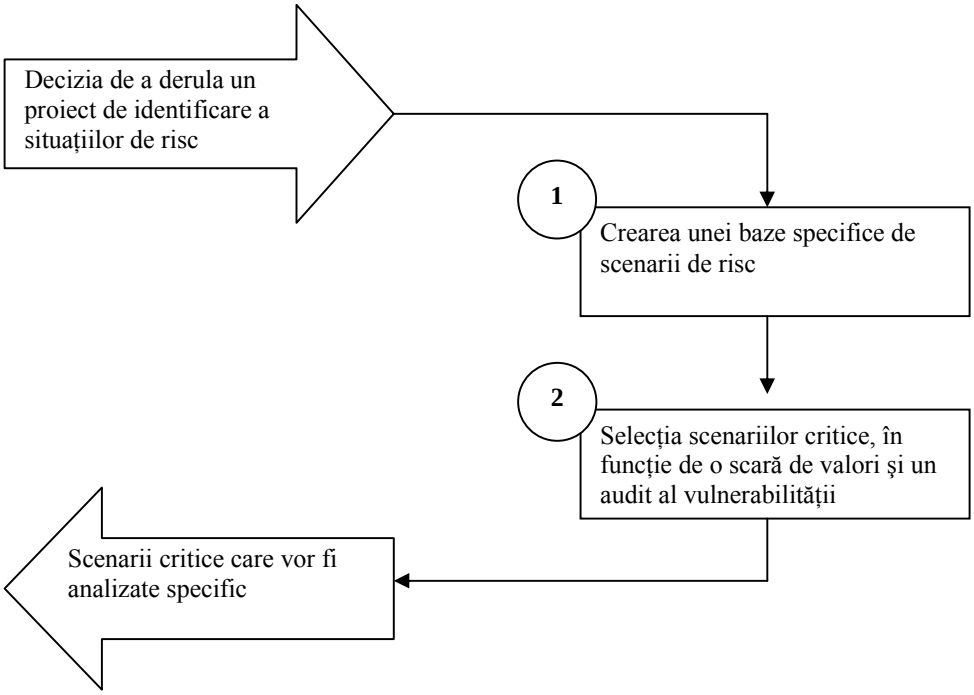


Figura 2: Identificarea situațiilor de risc

3.2 Crearea unui baze de scenarii specifice

O bază de scenarii specifice poate fi derivată din scenariile generice care fac parte din baza de cunoştințe MEHARI.

3.2.1 Baza de scenarii de risc generice

Bazele de cunoştințe MEHARI cuprind o bază de scenarii care a fost deja discutată în capitolul anterior.

Ea reprezintă un set de scenarii, clasificate prin familia tipului de consecință (în această versiune, există cam 170 de scenarii şi variantele lor clasificate în 12 familii). Pentru fiecare scenariu, există:

- descriere a consecințelor scenariului.
- descriere a cauzei şi originii scenariului.
- Tipul de eveniment caracteristic, pentru a evalua expunerea naturală.
- Tipul de bunuri implicat, pentru a evalua impactul intrinsec.
- Serviciile de securitate pertinente pentru scenariu, în funcție de rezultatul aşteptat (disuasiv, preventiv, protector, paliativ, sau recuperator).
- Formulele utilizate de procedurile automate pentru a calcula eficacitatea măsurilor de securitate pentru scenariu.
- Indicatorii globali ai tipului de consecință (A, I sau C, pentru Disponibilitate, Integritate, sau Confidențialitate), ai naturii evolutive (sau nu) a scenariului, şi tipurile de cauză (A, E sau V, pentru Accident, Eroare sau Act voluntar). Aceşti indicatori sunt folosiți şi de

procedurile automate pentru a calcula potențialitatea şi reducerea impactului (pentru tabelele de evaluare selectate folosite).

În plus, baza de cunoştințe include, pentru fiecare scenariu, un asistent de analiză (numit abordarea globală). Acesta este compus din definiții adaptate la fiecare tip de măsură de securitate, şi comentarii pentru a evalua direct eficacitatea măsurilor de securitate.

3.2.2 Personalizarea scenariilor ca funcție a bunurilor implicate

După cum s-a descris anterior, scenariile generice din MEHARI acoperă doar bunurile implicate prin raportarea lor pe tip, la un nivel relativ global. Se poate dori diferențierea fiecărui scenariu, în funcție de bunurile implicate.

În mod deosebit, dacă o clasificare a fost făcută pentru fiecare set de servere sau alte bunuri IT, şi fiecare set de date specifice pentru fiecare domeniu de aplicare, este tentant să se analizeze fiecare scenariu de tot atâtea ori câte domenii de aplicare există. Cu alte cuvinte, să se creeze tot atâtea ipostaze de scenarii câte domenii de aplicare sunt.

Să luăm, ca exemplu, unul din scenariile generice MEHARI, care este „furarea datelor prin accesul la sistem şi copierea fişierelor, de un hacker". Este posibil să se creeze ipostaze separate ale aceluiaşi scenariu pentru tipuri diferite de date (Resurse umane, vânzări, şi aşa mai departe). Acest lucru ar implica crearea, de la scenariul generic, a scenariilor specifice pentru fiecare set de bunuri pentru care a fost făcută o clasificare.

Această abordare este posibilă, şi foloseşte ceea ce noi am numit mai devreme în acest document „Descompunere Cartografică".

Acest lucru ar putea duce la un număr considerabil de scenarii; şi ar trebui avut grijă la folosirea acestei abordări pentru a nu complica viața inutil.

În practică, abordarea MEHARI de bază constă în folosirea unui scenariu generic doar cu un tip de bunuri general, raportat la scenariu, şi a cărui sensibilitate este luată din tabelul impactului intrinsec.

Această simplificare poate fi justificată de faptul că motivul pentru această analiză este identificarea căror situații de risc ar putea fi critice şi vor necesita o analiză mai detaliat. Va identifica care scenariu poate implica ce bunuri având ce nivel de sensibilitate.

3.2.3 Luarea în considerare a soluțiilor de securitate specifice

În identificarea căror scenarii ar putea fi critice, soluțiile de securitate existente folosite vor avea, desigur, o influență. Cu cât aceste soluții sunt mai eficiente, cu atât mai puțin critic va fi scenariul.

De aceea este clar că acele scenarii pentru care există, de exemplu, diferite medii sau sisteme, sau – mai general – diferite tipuri de soluții de securitate, ar trebui tratate separat. Asta este exact aceeaşi abordare folosită şi în timpul unui audit şi ***schema care a fost folosită pentru audit ar trebui re-folosită pentru a selecta situațiile critice de risc***.

Un alt mod de a aplica schema de audit la selectarea scenariilor critice este să se ia în considerare că, pentru a face selecția, vom baza selecția pe rezultatele auditului de securitate. Dacă de aceea, în timpul auditului, s-a considerat important să se distingă între diferite ipostaze, atunci ar trebui luate în considerare la fel de multe scenarii (diferite ipostaze ale scenariului generic) în timpul procesului de selecție după cum este necesar. În acest mod, diferitele servicii de securitate implicate în scenariu pot fi tratate separat, şi evaluate independent de altele.

Ar trebui reținut faptul că acest lucru ar putea crea foarte rapid un număr mare de scenarii. O schema de audit foarte simplă[6] poate duce la multiplicarea numărului de scenarii generice cu un factor destul de mare.

3.3. Evaluarea automată a scenariilor

Procedurile automate MEHARI au fost descrise în capitolul anterior.

Aceste proceduri automate folosesc rezultatele unui audit de securitate (şi, mai ales, schema de audit folosită pentru a construi baza de scenarii specifice).

Procedurile automate sunt folosite pentru a evalua STATUS-ul detaliat şi, în funcție de potențialitate şi de impactul intrinsec al fiecărui scenariu, potențialitatea şi impactul care rezultă pentru fiecare scenariu.

Gravitatea globală pentru fiecare scenariu şi criticalitatea acestuia (sau nu) poate deci fi dedusă dintr-un tabel de acceptabilitate a riscului.

3.4. Selectarea scenariilor critice care ar trebui luată în considerare în timpul analizei riscului

Începând cu baza de scenarii specifice, şi evaluarea automată a gravități lor, devine uşor să se selecteze scenariile critice; adică, acele scenarii care ar trebui luate în considerare într-o analiză a riscului făcută folosind procesul descris în capitolul anterior.

Scenariile a căror gravitate este peste un anumit nivel vor fi selectate pentru analiză. De obicei, scenariile cu o gravitate de 3 sau mai mare (pe o scară de la 1 la 4) sunt selectate, dar nu este nici o regulă stabilită.

Notă:

Dat fiind prudența recomandată în secțiunea anterioară privind evaluarea automată, recomandăm folosirea unui tabel al acceptabilității riscului relativ sever pentru selecția automată. Efectiv, tabelul acceptabilității riscului poate fi diferit la nivelul de selecție al scenariului critic de cel folosit în judecata finală a gravității unei situații de risc.

[6] De exemplu, o unitate organizațională, două tipuri de locații regionale (sediul central şi agenția regională), două tipuri de premise (tehnică şi IT pe de o parte, şi altele, zone de birouri, pe cealaltă parte), un singur tip de rețea cu o singură operare a rețelei, 2 tipuri de sistem (mainframe şi sisteme deschise) cu o singură operare IT, 2 tipuri de aplicații (unul pe mainframe şi unul pe sistemul deschis) şi 2 tipuri de dezvoltare (mainframe şi sisteme deschise).

Un tabel relativ sever pentru gravitate, precum cel arătat mai jos, ar putea fi folosit.

I = 4	3	3	4	4
I = 3	2	3	3	4
I = 2	1	2	3	3
I = 1	1	1	1	3
	P = 1	P = 2	P = 3	P = 4

Important:

În general, considerăm că scenariile cu o gravitate de nivel 4 sunt insuportabile, că acelea cu o gravitate de nivel 3 sunt inadmisibile şi cele cu niveluri mai joase de gravitate sunt tolerabile.

Anexa 1: Tabelul expunerii naturale standard

	Evaluarea expunerii naturale Evaluarea potențialității evenimentelor enumerate mai jos	**Foarte improbabil**	**Destul de improbabil**	**Destul de probabil**	**Foarte probabil**	**Statu-Expo**
Accidente						
AC01	Scurt-circuit: fie cablu de alimentare sau echipament.		**X**			**2**
AC02	Fulger		**X**			**2**
AC03	Incendiu: origine internă: coş de gunoi, scrumieră, etc.		**X**			**2**
AC04	Accidente datorate apei sau lichidelor (scurgerea unei țevi, lichid vărsat accidental, etc.)		**X**			**2**
AC05	Inundație datorată unei țevi sparte sau care curge		**X**			**2**
AC06	Inundație datorată creşterii apei râului sau de adâncime		**X**			**2**
AC07	Inundație datorată stingerii unui incendiu în apropiere		**X**			**2**
AC08	Pană de curent de lungă durată datorată unei cauze externe		**X**			**2**
AC09	Nedisponibilitatea locației: interzicere decisă de autorități (risc de poluare, răscoală, etc.)		**X**			**2**
AC10	Pierderea personalului strategic		**X**			**2**
AC11	Defectarea echipamentului auxiliar (alimentarea cu energie, aer condiționat, etc.)		**X**			**2**
AC12	Defectarea echipamentului IT sau telecom		**X**			**2**
AC13	Defectarea hardware a unui echipament IT sau telecom care nu poate fi rezolvată de întreținere sau furnizorul de întreținere este nedisponibil		**X**			**2**
AC14	Impas software care nu poate fi rezolvat de întreținere: editorul sau furnizorul de întreținere este nedisponibil		**X**			**2**
AC15	Saturarea accidentală a resurselor (CPU, memorie, disc, etc.)			**X**		**3**
AC16	Accident în timpul operării, rezultând în distorsionarea datelor			**X**		**3**
AC17	Datele sau configurarea şterse sau poluate de un virus			**X**		**3**
AC18	Pierderea accidentală a fişierelor de date cauzată de un proces automat			**X**		**3**
AC19	Pierderea accidentală a fişierelor de date cauzată de învechire, poluare, etc.		**X**			**2**
AC20	Pierderea accidentală a fişierelor de date cauzată de defectarea echipamentului (stricarea dischetei, etc.)		**X**			**2**
Reavoință						
MA01	Vandalism din afară: gloanțe sau obiecte aruncate din stradă, etc.		**X**			**2**
MA02	Vandalism din interior: de persoane autorizate în locație (personal, subcontractor, etc.).		**X**			**2**
MA03	Terorism: sabotaj, exploziv lăsat în apropierea locațiilor sensibile	**X**				**1**
MA04	Saturarea malițioasă şi repetată a resurselor IT de un grup de utilizatori		**X**			**2**
MA05	Saturarea rețelei cauzată de un vierme		**X**			**2**
MA06	Ştergerea malițioasă (direct sau indirect) a software-ului de pe unitatea de depozitare		**X**			**2**
MA07	Modificarea malițioasă (directă sau indirectă) a funcționalităților unui program sau a operării unui			**X**		**3**
MA08	Introducerea datelor distorsionate sau modificarea datelor			**X**		**3**
MA09	Accesul intenționat la date sau informații şi dezvăluirea informațiilor			**X**		**3**

MA10	Diversiunea fişierelor sau furtul mediilor de date			**X**		**3**
MA11	Ştergerea intenționată (directă sau indirectă) furtul sau distrugerea recipientelor de date sau programe			**X**		**3**
MA12	Furtul PC-ului portabil în afara locației organizației			**X**		**3**
MA13	Ştergerea malițioasă a configurărilor de rețea		**X**			**2**
MA14	Ştergerea malițioasă a configurărilor de sistem sau aplicații		**X**			**2**
MA15	Diversiunea codului sursă a programului		**X**			**2**
MA16	Spionarea de un stat străin sau mafia (folosind resurse importante)	**X**				**1**
MA17	Furtul echipamentului IT sau de rețea, în cadrul organizației			**X**		**3**
Acțiuni intenționate deşi nu malițioase						
AV01	Absența sau greva personalului operațional IT		**X**			**2**
AV02	Plecarea sau demisia personalului strategic			**X**		**3**
AV03	Intruziunea în resursele IT a unei părți terțe, inițiată de organizație sau de personalul acesteia			**X**		**3**
AV04	Utilizarea ilegală a software-ului sau produselor cu licență			**X**		**3**
Erori						
ER01	Retrogradarea neintenționată a performanțelor, rezultând din o operațiune de întreținere		**X**			**2**
ER02	Ştergerea neintenționată a programului de software din întâmplare sau eroare umană			**X**		**3**
ER03	Alterarea neprevăzută a datelor în timpul operațiunii de întreținere			**X**		**3**
ER04	Eroarea în timpul introducerii datelor				**X**	**4**
ER05	Bug al sistemului de operare, pachetului middleware sau software				**X**	**4**
ER06	Bug în programul de aplicație				**X**	**4**
ER07	Eroare introdusă în timpul modificării funcțiilor sau a macro în spreadsheet			**X**		**3**

Anexa 2 : Definiția nivelurilor de expunere naturală

Expunerea naturală la risc

- Nivelul 1 : Expunere foarte mică
  - Independent de orice măsuri de securitate, probabilitatea ca un scenariu dat va avea loc este foarte mică şi practic neglijabilă.
- Nivelul 2 : Expunere mică (abia expus).
  - Chiar şi fără orice măsuri de securitate, combinația dintre mediu (cultural, uman, geografic sau altul) şi context (strategic, competitiv, social, …) fac ca probabilitatea ca un scenariu dat să aibă loc, în termen scurt sau mediu, foarte mică.
- Nivelul 3 : Expunere medie (nu deosebit de expus)
  - Mediul şi contextul întreprinderii sunt de aşa natură încât, dacă nu se face nimic pentru a-l evita, scenariul dat este menit să se producă în termen mai mult sau mai puțin scurt.
- Nivelul 4 : Expunere mare : (deosebit de expus).
  - Mediul şi contextul întreprinderii sunt de aşa natură încât, dacă nu se face nimic pentru a-l evita, producerea scenariului dat este probabil să aibă loc în termen foarte scurt.

Anexa 3 : Tabelul impactului intrinsec

Clasificarea nivelului datelor, informațiilor şi componentelor de infrastructură		A	I	C
Date şi Informații				
D01	Fişiere de date sau baze de date accesate de aplicații			
D02	Fişiere office şi date comune			
D03	Fişiere office personale (pe PC, etc.)			
D04	Informații şi date printate sau scrise păstrate de utilizatori şi arhive personale			
D05	Listări sau documente printate			
D06	Mesaje trimise, vizualizări de monitor, etc. (date parțiale)			
D07	Mailuri şi faxuri			
D08	Arhive patrimoniale sau documente folosite ca dovezi			
D09	Date şi informații publicate pe site-uri publice sau interne			
Infrastructură : telecomunicații şi sisteme				
R01	Echipamente şi linkuri Wide Area Network (sisteme de rețea şi software asociat)			
R02	Echipamente şi linkuri Local Area Network (sisteme de rețea şi software asociat)			
R03	Date de configurare WAN			
R04	Date de configurare LAN			
S01	Sisteme principale, servere care găzduiesc aplicații şi echipamentele lor periferiale, servere de fişiere comune			
S02	Fişiere de configurare legate de sistemele şi serverele principale			
S03	Stații de lucru şi terminale ale utilizatorilor (PC, imprimante locale, periferice, interfețe specifice, etc.)			
A01	Software, pachet sau middleware de aplicații (cod executabil)			
A02	Cod sursă			
A03	Fişiere de configurare legate de aplicații			
A04	Software şi aplicații ale utilizatorului sau clientului			
Infrastructură generală				
E01	Spațiul de lucru şi mediul utilizatorului			
E02	Echipamente folosite pentru schimburi vocale (telefon, etc.)			
I01	Totalitatea camerei computerelor şi locația telecom			
Impacturi intrinseci (obiecte globale sau nelegate de un obiect anume)				
Pierderea sau distrugerea completă a unui utilaj				
Nedisponibilitatea personalului				
P01	Echipe de specialişti (legat de afaceri)			
P02	Personalul de operațiuni IT			
Neconformarea legală sau reglementatoare				
C01	Neconformarea la legile şi reglementările legate de protecția vieții private			
C02	Neconformarea la legile şi reglementările legate de controalele financiare			
C03	Neconformarea la legile şi reglementările legate de drepturile de proprietate intelectuală			
C04	Neconformarea la legile şi reglementările legate de protecția sistemului informațional			
C05	Neconformarea la legile şi reglementările legate de punerea în pericol al personalului şi siguranța publică şi a mediului			

Anexa 4: Definiția nivelurilor factorilor de reducere a riscului

Măsuri disuasive

- Nivelul 1: Efectul măsurilor disuasive este mic sau zero.
  - Potențialul atacator poate considera în mod logic că el sau ea nu se supune nici unui risc personal. Ei consideră că nu vor fi identificați, sau vor avea posibilitatea de a folosi argumente puternice pentru a refuta orice acuzație privind acțiunile efectuate, sau că orice pedeapsă va fi uşoară.
- Nivelul 2: Efectul măsurilor disuasive este mediu.
  - Potențialul atacator poate considera în mod logic că el sau ea se supune doar unui risc mic. În orice caz, orice prejudiciu personal potențial va fi suportabil.
- Nivelul 3: Efectul măsurilor disuasive este mare.
  - Potențialul atacator poate considera în mod logic că el sau ea se supune uni risc mare. Ar trebui să realizeze că vor fi identificați cu siguranță, şi că pedeapsa va fi gravă.
- Nivelul 4: Efectul măsurilor disuasive este foarte mare.
  - Potențialul atacator poate considera în mod logic că el sau ea ar trebui să abandoneze orice idee de a efectua acțiunea. Ar trebui să realizeze că vor fi identificați cu siguranță, şi că orice pedeapsă care rezultă va depăşi cu mult orice câştig potențial.

Măsuri preventive

- Nivelul 1: Efectul măsurilor preventive este mic sau zero.
  - Orice persoană din organizație, sau din apropierea ei, sau chiar cineva care ştie ceva despre ea, este capabilă să pună acest scenariu în mişcare, cu mijloacele pe care le au la dispoziție (sau sunt uşor de obținut).
  - Circumstanțe perfect obişnuite pot fi cauza acestui scenariu (utilizare necorespunzătoare, condiții obişnuite nefavorabile).
- Nivelul 2: Efectul măsurilor preventive este mediu.
  - Un profesionist poate porni scenariul, fără necesitatea mijloacelor sau uneltelor speciale în afară de cele disponibile în profesie.
  - Circumstanțe naturale rare pot produce acelaşi rezultat.
- Nivelul 3: Efectul măsurilor preventive este mare.
  - Doar un specialist, sau un profesionist cu unelte sau mijloace speciale, sau un grup de profesionişti în înțelegere şi care folosesc mijloacele şi uneltele lor colective ar putea reuşi.
  - De obicei este rezultatul conjuncției a circumstanțelor rare sau excepționale.
- Nivelul 4: Efectul măsurilor preventive este foarte mare.
  - Doar câțiva experți hotărâți, cu mijloace excepționale, ar putea reuşi.
  - Doar conjuncția circumstanțelor foarte rare sau excepționale ar permite ca acest scenariu să aibă loc.

Măsuri protectoare sau restrângere

- Nivelul 1: Efectele restrângerii şi limitarea consecinţelor directe sunt foarte mici sau zero.
    - Fie daunele şi consecinţele lor directe nu pot fi limitate, sau nu vor fi detectate pentru ceva timp. Măsurile protectoare posibile au atunci doar o influenţă restrânsă asupra nivelului consecinţelor directe.
- Nivelul 2: Efectele restrângerii şi limitarea consecinţelor directe sunt medii.
    - Chiar dacă dauna şi consecinţele sale directe pot fi limitate, timpul pentru a le detecta este lung, sau reacţia este înceată. Măsurile protectoare care sunt folosite au o influenţă reală asupra rezultatului, dar consecinţele directe sunt încă foarte mari.
- Nivelul 3: Efectele restrângerii şi limitarea consecinţelor directe sunt mari.
    - Evenimentul este detectat rapid, cu reacţie imediată.
    - Măsurile protectoare care sunt folosite au o influenţă reală asupra impactului direct, care rămâne real dar limitat în scop şi administrabil.
- Nivelul 4: Măsurile au un efect foarte puternic.
    - Începutul scenariului este detectat în timp real, înainte ca să poată fi făcută vreo daună reală, şi măsurile protectoare sunt puse în funcţiune imediat.
    - Consecinţele directe sunt limitate la deteriorări mici imediate datorită accidentului, erorii sau acţiunii voluntare.

Măsuri paliative

- Nivelul 1: Efectele limitării consecinţelor indirecte sunt foarte mici sau zero.
    - Fie sunt folosite măsuri total improvizate, sau se consideră că efectul lor va fi mic.
- Nivelul 2: Efectele limitării consecinţelor indirecte sunt medii.
    - Măsurile paliative sau de ajutorare au fost planificate în mare, dar detaliile fine lipsesc. Se poate considera că, datorită lipsei de detalii, va exista o lipsă corespondentă de eficienţă a măsurii paliative. Timpul pentru a restabili operaţiunile normale nu poate fi prezis cu siguranţă, sau nu va schimba fundamental natura daunei cauzate.
- Nivelul 3: Efectele limitării consecinţelor indirecte sunt mari.
    - Nu numai că măsurile paliative au fost planificate şi organizate bine, ci au fost şi testate şi validate.
    - Timpul pentru a restabili operaţiunile normale poate fi estimat sau ştiut precis, şi este de aşa natură încât va reduce considerabil gravitatea consecinţelor indirecte ale scenariului
- Nivelul 4: Efectele limitării consecinţelor indirecte sunt într-adevăr foarte mari.
    - Operaţiunile normale continuă fără nici o întrerupere observabilă.

Măsuri recuperatoare

- Nivelul 1: Efectul măsurilor recuperatoare este mic sau zero.
  - Ceea ce poate fi recuperat prin asigurări sau procese legale nu este nimic în comparație cu daunele cauzate de impactul global al scenariului şi consecințele sale.
- Nivelul 2: Efectul măsurilor recuperatoare este mediu.
  - Ceea ce poate fi recuperat nu este neglijabil, dar organizația are responsabilitatea pentru cea mai mare parte a impactului scenariului. În cazul unui incident major, nu este sigur că transferul riscului ar permite organizației să continue operațiunile.
- Nivelul 3: Efectul măsurilor recuperatoare este mare.
  - Ceea ce este recuperat prin asigurări sau procese legale este suficient pentru a atenua serios impactul scenariului. În orice caz, operațiunile pot continua.
  - Impactul rezidual ar fi, foarte grav, dar nu ar atinge nivelul « Vital ».
- Nivelul 4: Efectul măsurilor recuperatoare este extrem de mare.
  - Oricât de grav ar fi dezastrul, impactul rezidual rămâne suportabil (nivelul 2).

Anexa 5: Principii pentru construirea tabelelor de evaluare STATUS

Principiile descrise mai jos sunt cele care au fost folosite pentru a crea tabelele STATUS-P şi STATUS-RI pentru transformarea STATUS-ului detaliat în STATUS global.

Tabelul de evaluare STATUS-P

Tabelul se bazează pe următorul raționament:

- Expunerea naturală fiind definită ca fiind evaluarea potențialității intrinseci fără nici o altă măsură, valoarea maximă a STATUS-P este cea a STATUS-EXPO (în absența oricărei alte măsuri, şi anume, dacă STATUS-DISS şi STATUS-PREV au ambele o valoare de 1)
- Dacă valoarea STATUS-PREV este 3 sau 4, pentru accidente sau erori; atunci STATUS-P are o valoare maximă de 2 sau 1, respectiv.
- Dacă valoarea STATUS-PREV este 4, pentru acțiune voluntară; atunci STATUS-P are o valoare maxim de 2
- Dacă valoarea STATUS-PREV este 4, pentru acțiune voluntară; şi dacă expunerea este mai mică sau egală cu 3, atunci STATUS-P are o valoare maximă de 1.

Pe acest raționament au fost construite tabelele bazei de cunoştințe standard MEHARI.

Tabelul de evaluare STATUS-RI

Tabelul se bazează pe următorul raționament:

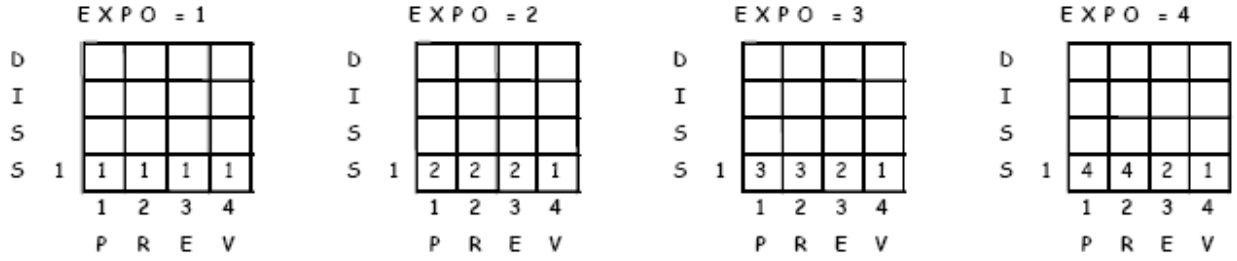
- Dacă valoarea lui STATUS-RECUP este 3, atunci valoarea lui STATUS-RI este cel puțin 2
- Dacă valoarea lui STATUS-RECUP este 4, atunci valoarea lui STATUS-RI este cel puțin 3
- Dacă valoarea lui STATUS-RECUP este 3 sau 4, pentru scenarii de disponibilitate, atunci valoarea lui STATUS-RI este cel puțin 3 (dacă planificarea de ajutorare este planificată corespunzător, atunci impactul care rezultă nu poate fi grav).
- Dacă valoarea lui STATUS-PROT este 4 într-un scenariu de integritate, totul poate fi evitat dacă restaurarea rapidă este posibilă, şi deci STATUS-RI este aliniat la valoarea lui STATUS-PALL, care, în acest caz, se ocupă de restaurare.
- Dacă valoarea lui STATUS-PROT este 3 într-un scenariu de integritate, dacă restaurarea rapidă este posibilă (STATUS-PALL = 3 sau 4), fără îndoială că ceea ce era mai rău a fost evitat, dar situația poate încă să fie foarte gravă: STATUS-RI = 2. Totuşi, dacă restaurarea rapid nu este posibilă (STAUS-PALL = 1 sau 2), nimic nu este atenuat, şi STATUS-RI = 1.
- Dacă valoarea lui STATUS-PROT este 1 sau 2 într-un scenariu de integritate, atunci valoarea lui STATUS-RI este 1, decât dacă o acțiune planificată nu este identificată în STATUS-RECUP (protecție mică fără măsură paliativă, deoarece acestea sunt compuse doar din măsuri fortifiante care nu au nici un efect asupra consecințelor directe, şi doar măsurile fortifiante joacă un rol)

Pe acest raționament au fost construite tabelele bazei de cunoştințe standard MEHARI.

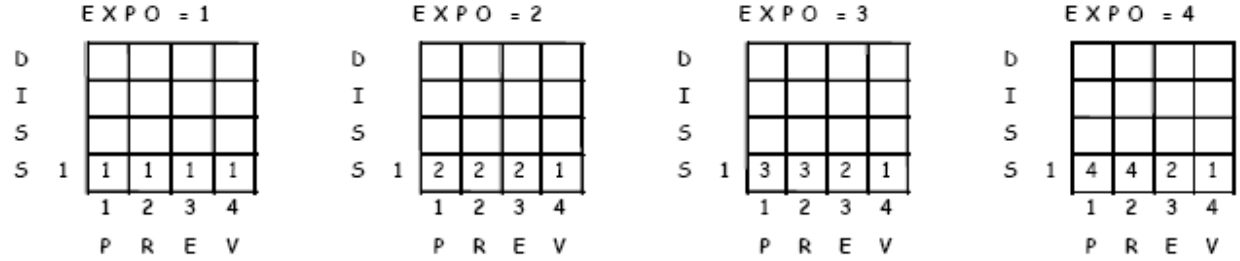
Anexa 6 : Tabele standard de evaluare

Grile de evaluare pentru STATUS-P pentru scenariu care rezultă din:

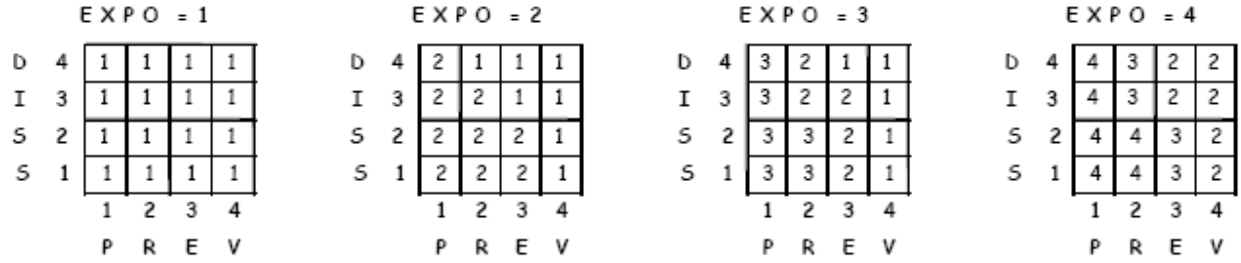
1. Un accident



2. O eroare



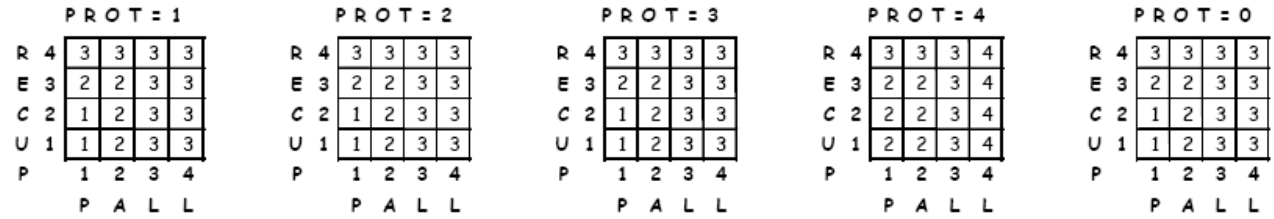
3. O acțiunea răuvoitoare



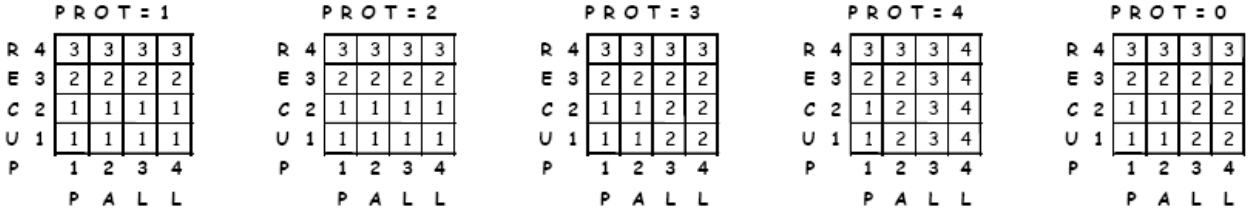
Grile de evaluare pentru STATUS-RI (Reducerea impactului)

Scenariile ne-evoluționare sunt reprezentate ca PROT = 0.

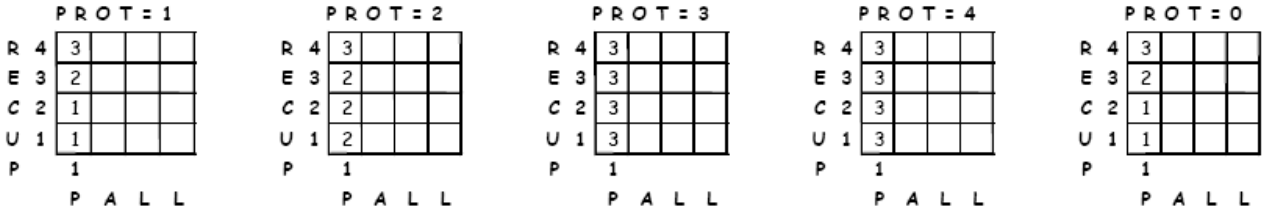
1. Scenarii care afectează Disponibilitatea (A)



2. Scenarii care afectează Integritatea (I)



3. Scenarii care afectează Confidențialitatea (C)



Anexa 7: Cerințe speciale de securitate

După ce s-a evaluat gravitatea unui set de situații de risc şi s-au folosit rezultatele auditului serviciilor de securitate[7], este posibil să se exprime cerințele de securitate ca o evaluare a nevoilor consolidate, urmate de ordonarea lor a priorității.

Această abordare foloseşte definiția "**cerințelor serviciului**" după cum este descris mai jos.

Cerințele serviciului

O cerință a serviciului de securitate este definită pentru fiecare scenariu, folosind următoarele principii de bază.

Cerința serviciului pentru un scenariu dat

Un serviciu de securitate dat poate avea o influență asupra gravității unui scenariu. **Dacă acesta este cazul, atunci o cerință de securitate există pentru acest serviciu pentru scenariu.**

Cantitativ, cerința serviciului va fi chiar mai importantă decât:
- influența sa (reprezentată de *factorul său de influență*), pentru acest scenariu, va fi foarte mare;
- gravitatea scenariului va fi considerată mare;
- calitatea actuală a serviciului va fi mică.

Deci, pentru serviciul i confruntat cu scenariul k, cerința serviciului poate fi calculată de formula:

$$BS_{ik} = e_{ik} * b^{G}_{k} * (4 - \sigma_i)$$

Unde:

BS_{ik} = cerința serviciului pentru serviciul i pentru scenariul k
e_{ik} = coeficientul de influență al serviciului i pentru scenariul k
b = parametrul de sensibilitate
G_k = gravitatea scenariului k
σ_i = calitatea serviciului de securitate i

Coeficientul de influență "e", cu o valoare între 0 şi 16, reprezintă gradul de influență al serviciului de securitate asupra scenariului.

Este dedus din formula folosită de MEHARI pentru a evalua eficacitatea diferitelor tipuri (disuasiv, preventiv, protector, paliativ, sau recuperator) de măsuri asupra scenariului.

Acest coeficient este calculat folosind formula de mai jos:
$e_{ik} = \alpha_{ik} \cdot \beta_{ik}$

[7] Un serviciu de securitate al MEHARI are de obicei o sferă mai mare decât un Control ISO 17799.

Dacă serviciul este atribuit doar pentru un tip de măsură, valoarea lui α_{ik} este stabilită în acest mod:

- Dacă serviciul este singurul care va fi folosit pentru tipul de măsură luată în considerare, $\alpha_{ik} = 2$
- Dacă serviciul este folosit de o formulă de tipul min (serv_A; serv_B) $\alpha_{ik} = 2$
- Dacă serviciul este folosit de o formulă de tipul max (serv_A; serv_B) $\alpha_{ik} = 1$

În cazul unei formule complexe, doar funcția ("min" sau "max") care atribuie direct acest serviciu de securitate va fi luată în considerare.

Valoarea lui β_{ik} este determinată de faptul dacă serviciul de securitate I are:

- o influență disuasivă pentru scenariul k, $\beta_{ik} = 4$
- o influență preventivă pentru scenariul k, $\beta_{ik} = 8$
- o influență protectoare pentru scenariul k, $\beta_{ik} = 4$
- o influență paliativă pentru scenariul k, $\beta_{ik} = 8$
- influență recuperatoare pentru scenariul k, $\beta_{ik} = 2$

Dacă serviciul de securitate este folosit pentru mai multe tipuri de măsuri, vor fi calculați la fel de mulți coeficienți de influență, şi cea mai mare valoare a coeficientului de influență ca fi reținută.

b, care este folosit ca parametru de sensibilitate, pentru a ancora gravitatea fiecărui scenariu, are o mare influență asupra rezultatului final:

- valoarea de 2 minimalizează efectul gravității unui scenariu
- în general, o valoarea de 8 este considerată ca fiind o alegere bună.

Consolidarea cerințelor serviciului

Consolidarea cerințelor serviciului: BS_i pentru serviciul I, va fi evaluată prin suma simplă:

$$BS_i = \sum_k BS_{ik}$$

BS_i, cerința serviciului astfel calculată, are chiar o mai mare importanță decât serviciul folosit de mai multe scenarii, şi dacă aceste scenarii sunt grave, şi dacă serviciul poate influența gravitatea scenariilor.

Totuşi, alegerea de a îmbunătăți un serviciu poate fi inconsistentă cu alegerea făcută în organizație, la nivelul planificării strategice (dacă o politică de securitate a fost definită). MEHARI propune de aceea următoarea abordare:

- Sortați scenariile pentru a le arăta clar pe cele care necesită servicii de securitate cu cele mai mari cerințe globale;
- Analizați dacă aceste servicii de securitate sunt consistente cu directivele şi recomandările politicii de securitate globale. Orice răspuns negativ la acest nivel va pune inevitabil politica de securitate la îndoială.
- Dacă răspunsul este pozitiv, evaluați nivelul de calitate revizuit al fiecărui serviciu de securitate ca o funcție a îmbunătățirilor decise deja în ceea ce îl priveşte (adăugări

sau modificări la proceduri şi/sau mecanisme);
- Re-estimați gravitatea care rezultă şi noile cerințe ale serviciului;
- Luați-o de la capăt!

Pachetul software RISICARE[8] include automatisme pentru a urma acel proces.

[8] RISICARE este produs de BUC S.A.