



# MEHARI 2007

## **Analiza mizelor de joc și Ghidul Clasificării**

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

Vă rugăm să trimiteți întrebările și comentariile dumneavoastră la adresa [mehari@clusif.asso.fr](mailto:mehari@clusif.asso.fr)

# Cuprins

1	Introducere .....	4
2	Scara de valori a defecțiunilor .....	6
2.1	Identificarea principalelor activități și obiectivele lor .....	6
2.1.1	Rezultatele prevăzute.....	6
2.1.2	Abordare.....	6
2.2	Identificarea potențialelor defecțiuni .....	6
2.2.1	Rezultate prevăzute .....	6
2.2.1.1	Potențiale defecțiuni identificate la nivel funcțional .....	7
2.2.1.2	Potențialele defecțiuni identificate la nivel tehnic .....	8
2.2.2	Abordare.....	8
2.3	Analiza mizelor de securitate: evaluarea gravității defecțiunilor identificate.....	9
2.3.1	Scara gravității.....	9
2.3.2	Criteriile defecțiunii și praguri de criticalitate: rezultate elementare.....	10
2.3.3	Abordare.....	10
2.4	Scara de valori a defecțiunilor .....	10
3	Clasificarea informației și a bunurilor ajutoare .....	12
3.1	Identificarea elementelor care vor fi clasificate.....	12
3.1.1	Identificarea elementelor legate de procesele de afaceri .....	12
3.1.2	Identificarea elementelor legate de serviciile comune.....	15
3.1.3	Identificarea infrastructurii ajutoare comune care trebuie clasificată .....	15
3.2	Criteriile de clasificare .....	16
3.3	Procesul clasificării .....	16
3.3.1	Clasificarea bunurilor care sprijină procesele de afaceri .....	16
3.3.2	Clasificarea elementelor legate de serviciile comune.....	17
3.3.3	Clasificarea elementelor de infrastructură globală .....	17
4	Construirea tabelului impactului intrinsec.....	18
5	Sfaturi practice .....	20
5.1	Puncte importante care trebuie luate în considerare în crearea scării de valori.....	20
5.1.1	Concentrați-vă asupra aspectelor celor mai critice .....	20
5.1.2	Excluderea controalelor existente.....	20
5.1.3	Consistența defecțiunilor de diferite tipuri .....	20
5.1.4	Aspecte strategice și de luare a deciziilor ale scării de valori.....	20
5.2	Puncte importante în timpul clasificării.....	21
5.3	Limite pentru clasificare.....	21
5.4	Planuri de acțiune .....	21
Anexa 1:	Exemplu al unei scări de valori (întreprindere industrială).....	22
Anexa 2:	Tabelul Impactului Intrinsec .....	26

# 1 Introducere

Necesitatea unei analize a ceea ce este în joc pentru managementul riscului informațional a fost recunoscută în documentul „*Concepte și Mecanisme MEHARI*”.

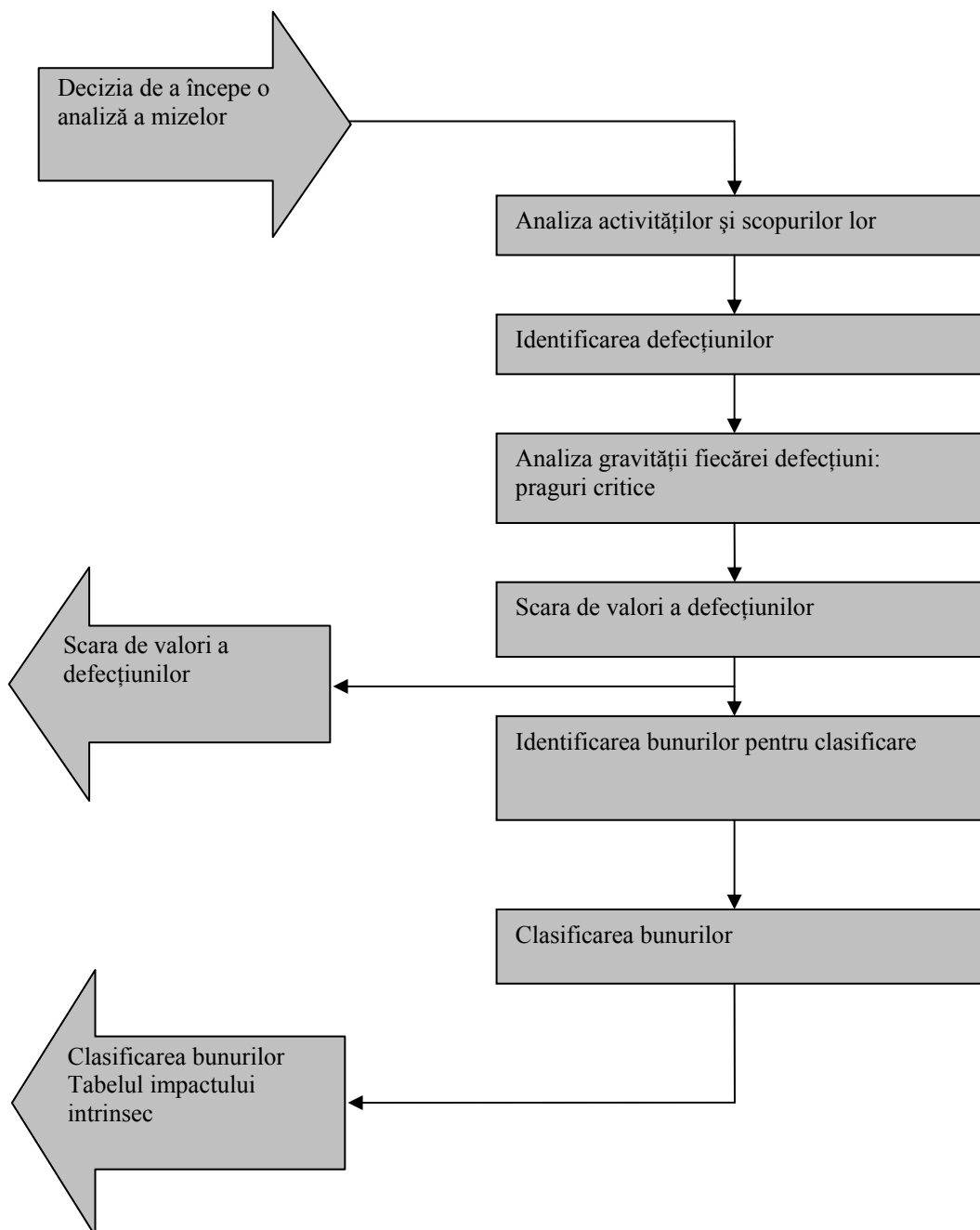
Această analiză trebuie să ofere două seturi principale de rezultate:

- Scara de valori a defecțiunilor,
- Evaluarea sau clasificarea bunurilor legate de informație.

Din aceste două seturi de rezultate, se poate deduce tabelul impactului intrinsec, folosit pentru evaluarea scenariilor de risc oferite de către MEHARI (vezi „*Ghidul MEHARI pentru Analiza Riscului*”).

Procedura pentru analiza mizelor este descrisă mai jos.

Abordarea MEHARI constă în analizarea activităților întreprinderii sau organizației, și astfel a proceselor sale de afaceri care au legătură cu informația, pentru a deduce ce defecțiuni ar putea avea loc, și să se evalueze cât de grave ar putea fi aceste defecțiuni. Apoi este posibil să se evalueze bunurile legate de informație.



## 2 Scara de valori a defecțiunilor

Acest proces este conceput pentru a oferi o scară de valori pentru defecțiunile care ar putea afecta semnificativ activitățile unei entități<sup>1</sup>.

Analiza cuprinde patru stadii:

- Analiza principalelor activități și scopurile lor
- Identificarea defecțiunilor posibile pentru fiecare activitate, care poate fi realizată la următoarele nivele:
  - Tehnic,
  - Funcțional.
- O evaluare a nivelului gravității defecțiunilor, activitate cu activitate,
- Determinarea unei scări globale a valorilor pentru entitate.

### 2.1 Identificarea principalelor activități și obiectivele lor

Un bun punct de plecare este identificarea principalelor activități ale domeniului care este analizat, descrierea lor, și identificarea scopurilor lor sau cel puțin rezultatele prevăzute.

#### 2.1.1 Rezultatele prevăzute

Activitățile vor fi descrise în termeni funcționali.

Pe lângă o descriere funcțională, merită să se definească rezultatele prevăzute sau scopurile activității. Aceste rezultate dorite ar trebui definite din punctul de vedere al entității, și din acela al entităților „client”.

Iată un exemplu:

<i>Funcție</i>	<i>Scopuri și rezultate prevăzute</i>
Creează și mențin o perspectivă consolidată a trezoreriei și a necesităților ei.	Permite departamentului de contabilitate să suplimenteze contabilitatea după necesități (și să evite plățile nesuținute).

#### 2.1.2 Abordare

O identificare riguroasă și exhaustivă a activităților poate fi făcută printr-o analiză a procesului în care acționează acestea. Acest lucru presupune identificarea tuturor proceselor din domeniul examinat, chiar și sub-împărțirea lor în câte sub-procese este necesar pentru a evidenția diferitele dependențe și rezultate intermediare.

Experiența arată că o abordare globală și mai intuitivă, dacă are un nivel destul de ridicat de sponsorizare a managementului, poate identifica rapid principalele funcții și scopurile lor. Acest lucru este suficient pentru necesitățile acestei abordări.

*Abordarea este astfel bazată pe interviuri individuale (între 60 și 90 de minute) cu manageri responsabili pentru diferite activități în întreprindere sau organizație.*

## 2.2 Identificarea potențialelor defecțiuni

După ce sunt identificate activitățile, defecțiunile potențiale sau cele suspectate asociate cu ele ar trebui aduse la lumină.

### 2.2.1 Rezultate prevăzute

Descrierea defecțiunilor ar trebui să fie de așa natură încât gravitatea să poată fi evaluată.

<sup>1</sup> Aceasta poate fi însăși compania sau o entitate operațională, pentru care sunt definite obiective de securitate, sau pentru un anumit proiect, unde riscurile specifice trebuie identificate.

Totuși, trebuie menționat că o defecțiune poate fi descrisă în mai multe moduri.

- La nivelul elementului care deranjează sau este deranjat în procesul care este examinat. Acesta ar putea fi, de exemplu, indisponibilitatea sistemului de management al trezoreriei sau baza de date asociată; deci, la nivel tehnic.
- La nivelul procesului însuși (la nivel funcțional). De exemplu, incapacitatea de a oferi o privire consolidată asupra necesităților trezoreriei.

Aceeași defecțiune poate astfel să fie descrisă fie în ceea ce privește indisponibilitatea datelor necesare pentru a produce un rezultat specificat, fie în ceea ce privește incapacitatea de a executa sarcina care ar produce rezultatul. Prima dintre acestea este cunoscută în MEHARI ca **analiza la nivel tehnic a mijelor de securitate**, iar cea din urmă este cunoscută ca **analiza funcțională a mijelor de securitate**.

### 2.2.1.1 Potențiale defecțiuni identificate la nivel funcțional

La nivel funcțional, scopul este identificarea potențialelor defecțiuni care au un impact semnificativ asupra activităților întreprinderii. Acestea vor fi de obicei defecțiuni ale proceselor. Următoarele criterii generice de profil ale defecțiunii procesului vor fi valabile de obicei:

- **Sincronizarea incorectă:** sarcinile sau activitățile care sunt planificate nu sunt terminate la timp;
- **Lipsa concordanței:** sarcinile sau activitățile care sunt planificate nu sunt terminate în conformitate cu specificațiile;
- **Lipsa completitudinii:** sarcinile sau activitățile planificate sunt terminate doar parțial (deși părțile terminate sunt conform cu specificațiile);
- **Lipsa corectitudinii:** sunt îndeplinite sarcini sau activități adiționale care nu erau planificate sau specificate;
- **Lipsa discreției:** informația este dezvăluită necorespunzător în timp ce sarcinile sau activitățile sunt îndeplinite;
- **Lipsa controlului:** sarcinile sau activitățile sunt îndeplinite și terminate după cum era planificat dar fără nici un control sau vizibilitate a execuției lor.

Este astfel posibil să se descrie o defecțiune în ceea ce privește sarcina sau activitatea implicată de către tipul de defecțiune.

De asemenea este deseori util să se descrie consecințele potențiale, pentru a înțelege mai bine gravitatea lor.

Astfel, folosind exemplul ipotetic al dezvăluirii necorespunzătoare a salariilor angajaților, merită să se identifice consecințele potențiale: acțiunea de grevă, obligația de a da numeroase mărimi de salariu pentru anumite categorii de personal, de-motivarea personalului, și așa mai departe.

De asemenea, dacă defecțiunea închipuită privește schimbările la plată, merită identificarea faptului dacă consecințele potențiale implică sau nu fraudă și pierderea de bani, sau acțiunea de grevă din partea personalului (sau de-motivarea acestora), sau necesitatea de a face corecții numeroase și complicate.

***Fiecare defecțiune, la nivel funcțional, ar trebui descrisă ca o schimbare în procesul de afacere. Astfel ea ar trebui descrisă în ceea ce privește procesul sau activitatea în cauză, precum și prin tipul de defecțiune și tipul potențialelor consecințe.***

Folosind exemplul managementului trezoreriei, menționat mai sus:

<i>Funcție</i>	<i>Scopurile și rezultatele așteptate</i>
Întârzierea plății în conturile trezoreriei	Incapacitatea de a plăti furnizorii, implicând o întrerupere a livrărilor și astfel a producției.

### 2.2.1.2 Potențialele defecțiuni identificate la nivel tehnic

La nivel tehnic, scopul este identificarea defecțiunilor semnificative în asigurarea bunurilor necesare pentru întreprindere sau organizație.

Bunurile care sunt asigurate ar putea fi:

- Bunuri fizice:
  - Bunuri obișnuite pentru orice întreprindere (spațiu pentru birouri, echipament pentru birouri, telefoane și faxuri, alt echipament mai specific, etc.);
  - Bunuri IT (servere, stații de lucru, rețele de date, etc.);
  - Bunuri documentare în general, și cele specifice pentru sarcină sau activitate;
  - Bunuri pentru comunicare (poșta, rețele de telefonie, etc.).
- Bunuri „soft”:
  - Date (fișiere, baze de date, elemente de referință specifice cerințelor activității);
  - Programe (software de bază, aplicații, etc.)
- Resurse umane și bunuri:
  - personalul necesar (competență, delegare și decizii, etc.).

Tipurile clasice de defecțiuni sunt **pierderea disponibilității, sau a integrității sau a confidențialității**. La fel ca pentru defecțiunile la nivel funcțional, și din aceleași motive, este deseori util să se descrie consecințele potențiale, pentru a înțelege mai bine gravitatea acestora.

***Defecțiunile tehnice identificate astfel vor fi descrise în ceea ce privește degradarea care ar putea avea loc la nivelul bunurilor folosite de către proces, și al consecințelor unei astfel de degradări.***

Folosind exemplul anterior al trezoreriei, obținem:

<i>Defecțiune</i>	<i>Consecințe</i>
Baza de date a trezoreriei indisponibilă Managementul bazei de date a trezoreriei indisponibil	Întârzieri ale plăților în conturi, care implică o incapacitate de a plăti furnizorii, care la rândul ei duce la întreruperea livrărilor și a producției.

#### **Notă:**

Exemplul folosit accentuează multiplicarea rezultatelor. O defecțiune dată poate, efectiv, să fie exprimată fie la nivel funcțional sau la nivel tehnic. Totuși, descrierile la nivel tehnic pot avea mai multe consecințe, și vor fi mai puțin durabile deoarece depind de tehnologiile care sunt folosite. Este de aceea preferabil să se dea prioritate descrierilor la nivel funcțional.

### 2.2.2 Abordare

Aici ar putea folosită din nou o abordare foarte sistematică, pe baza unei analize a procesului și a imaginării tuturor „deviațiilor” posibile din proces și sub-procese: rezultate incoerente, întârzieri în (sau absența) rezultate, indiscreție, etc.

Experiența arată că un nivel corespunzător al responsabilității în organizație va identifica rapid principalele defecțiuni printr-o abordare mai globală, care se reduce la a-i întreba pe manageri de ce se tem cel mai mult sau care este cea mai mare grijă a lor.

La nivel funcțional, ei cunosc procesul critic foarte bine. La nivel tehnic, chiar dacă nu pot face o listă exhaustivă cu aplicațiile și bazele de date folosite, pot cu siguranță să le descrie global folosind termeni generici care vor fi de ajuns („plată”, pentru acele programe și aplicații implicate, de exemplu).

***Descrierea defecțiunilor, fie la nivel funcțional sau tehnic, poate fi constituită astfel prin interviuri individuale, după cum s-a menționat anterior, cu managerii diferitelor activități din***

*întreprindere sau organizație.*

## **2.3 Analiza mizelor de securitate: evaluarea gravității defecțiunilor identificate**

A treia fază în determinarea scării de valori a defecțiunilor vrea să *evalueze gravitatea defecțiunilor identificate anterior*. Pentru a face asta, o scară standard a gravității ar trebui folosită ca referință.

### **2.3.1 Scara gravității**

MEHARI identifică 4 nivele de gravitate sau criticalitate. Acestea sunt notate de la 1 la 4. Definițiile lor generale sunt descrise mai jos:

#### **Nivelul 4: Vital**

La acest nivel, riscul potențial este foarte grav, și chiar și existența și supraviețuirea entității (sau cel puțin una din principalele sale activități) este în pericol.

Dacă o astfel de defecțiune ar avea loc, ar privi întreaga forță de muncă, și ar putea crede că slujbele lor sunt în pericol.

Pentru organizații, precum serviciile publice, ale căror funcție nu poate fi pusă la îndoială, acest nivel al gravității ar putea conduce la un transfer la alt departament guvernamental, sau la sectorul privat.

Pentru companiile comerciale, și în termeni financiari, merită luat în considerare faptul că o astfel de defecțiune ar genera pierderi de așa nivel încât acționarii s-ar retrage (și ar rezulta în scăderi drastice în prețul acțiunilor).

În medicina umană, acest lucru ar fi echivalent cu un accident sau o boală „extrem de gravă”, sau unde doctorii s-ar abține să se pronunțe.

Dacă organizația supraviețuiește unei astfel de defecțiuni, ar exista consecințe grave și durabile.

#### **Nivelul 3: Foarte grav**

Aceste defecțiuni sunt considerate foarte grave la nivelul entității, deși viitorul său nu ar fi supus riscului.

La acest nivel al gravității, întreg personalul (sau, cel puțin, o mare parte) este preocupat de condițiile de lucru și relațiile sociale, dar slujbele lor nu sunt supuse riscului.

În termeni financiari, acest lucru ar avea un impact foarte negativ asupra profiturilor pentru acea perioadă, deși nu s-ar înregistra o retragere masivă a acționarilor.

În ceea ce privește imaginea publică, acest nivel de defecțiune dăunează deseori imaginii organizației în așa măsură încât ar dura mai multe luni pentru a o reface, chiar dacă impactul financiar nu poate fi evaluat precis.

Accidentele care duc la luni întregi de dezordine organizațională pentru o întreprindere ar fi și ele evaluate la acest nivel.

#### **Nivelul 2: Grav**

Defecțiunile de la acest nivel ar avea un impact clar asupra operațiunilor entității, a rezultatelor ei sau a imaginii, dar sunt controlabile global.

Doar o parte limitată din personal ar fi implicată în relațiile cu consecințele defecțiunii, cu un impact semnificativ asupra condițiilor lor de muncă.

## Nivelul 1: Nesemnificativ

La acest nivel, orice daună care ar rezulta nu ar avea un impact semnificativ asupra rezultatelor sau imaginii entității, chiar dacă unii membri ai personalului sunt foarte implicați în restabilirea statului inițial.

### 2.3.2 Criteriile defecțiunii și praguri de criticalitate: rezultate elementare

Defecțiunile identificate nu au neapărat o singură și unică gravitate. Dimpotrivă, în multe cazuri defecțiunile trebuie caracterizate de unul sau mai mulți parametri care sunt esențiali pentru nivelul de gravitate.

De exemplu, o întârziere în terminarea unui proces este o defecțiune a cărei gravități ar depinde de obicei de întârzierea cantitativă și de numărul de oameni asupra cărora întârzierea a avut un impact.

***Pentru fiecare defecțiune, ar trebui definiți parametrii semnificativi, cu valorile pragului care mută defecțiunea de un nivel al gravității la altul.***

Criteriile criticalității și pragurile lor corespondente vor permite astfel evaluarea gravității fiecărei defecțiuni, de la defecțiunea care are un impact minimal, la una care este vitală pentru entitatea în discuție.

Ca un exemplu, și folosind studiul de caz de mai devreme, defecțiunea ar produce următorul tabel:

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
Incapacitatea de a menține conturile din bancă aprovizionate corespunzător, deoarece bazele de date ale trezoreriei nu sunt disponibile.	Durata: mai puțin de 4 ore	Durata: între 4 ore și 2 zile	Durata: mai mult de 2 zile	

### 2.3.3 Abordare

Identificarea criteriilor defecțiunilor și evaluarea pragurilor criticalității vor fi realizate în timpul interviurilor cu managerii operaționali din întreprindere. În timpul aceluiași interviu (având durata între 60 și 90 de minute) va fi definită și activitatea, precum și identificarea potențialelor defecțiuni, și determinarea criticalității ca funcție a parametrilor semnificativi.

***Rezultatele elementare ale fiecărui interviu vor consta deci într-o descriere a acestor activități, o descriere a potențialelor defecțiuni, și o evaluare a nivelului lor de gravitate.***

## 2.4 Scara de valori a defecțiunilor

Va fi realizată apoi o compilație a diferitelor rezultate pentru fiecare activitate.

Un exemplu parțial<sup>2</sup> este arătat mai jos, pentru o activitate HR.

<sup>2</sup> În exemplu, valorile și criteriile sunt folosite doar pentru a ilustra principiul, și nu ar trebui în nici un caz luate ca standarde pentru aplicarea în cazuri reale

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
Falsificarea datelor de plată, conducând la fraudă	Pierdere < 0.1 M€	Pierdere între 0.1 M€ & 1 M€	Pierdere între 1 și 10 M€	Pierdere > 10 M€
Dezvăluirea informațiilor personale	Dezvăluirea salariului unui angajat	Dezvăluirea tuturor salariilor angajaților	Dezvăluirea repetată a salariilor tuturor angajaților	
Plata târzie a salariilor	Întârziere < 2 zile	Întârziere între 2 și 15 zile	Întârziere > 15 zile	
Distrușgerea datelor de bază folosite pentru plata salariilor (calcul & parametri)	Ștergerea datelor recente (din ultima lună)	Ștergerea datelor din anul anterior	Ștergerea tuturor datelor, și a urmelor istorice	

După ce s-a examinat astfel fiecare activitate, compilarea rezultatelor va oferi scări de valori a defecțiunilor pentru fiecare activitate, și la nivel global, corporativ al organizației sau companiei.

Scara de valori rezultantă reprezintă doar o compilare documentară a tuturor tipurilor de defecțiuni și pragurile lor critice, și poate fi văzută ca un pas de formalizare. Experiența a demonstrat că compilarea tuturor tipurilor de defecțiuni, și pragurile lor critice, pot scoate la iveală discrepanțe care nu ar fi văzute la nivelul activităților individuale.

***Un pas de consolidare este deci necesar.***

În orice caz, orice concluzii sau obiecte de acțiune care pot fi deduse din scara de valori, sau o folosesc, vor fi luate în serios doar dacă scara de valori reflectă un adevărat consens al opiniei managerilor entității.

***Este de aceea foarte recomandat să existe o discuție adevărată, și să se caute un consens al opiniilor privind scara de valori, cu acordul managementului asupra ei.***

***Rezultatul final va fi o scară de valori a defecțiunilor validată.***

Un exemplu complet este dat în Anexa 1.

## 3 Clasificarea informației și a bunurilor ajutătoare

Scara de valori a defecțiunilor este rezultatul principal al analizei mizelor de securitate. Ea este direct legată de activitățile și procesele fundamentale ale întreprinderii sau organizației.

Acestea fiind spuse, mecanismele de analiză a riscului, și anumite abordări mai sistematice folosite pentru alegerea soluțiilor sau construirea planurilor de acțiune, necesită ca defecțiunile (exprimate inițial în termeni dependenți de activitate) să fie reformulate în termeni tehnici legați de sistemul informațional, în cel mai larg sens al cuvântului. Exemple sunt: pierderea confidențialității a anumitor baze de date, indisponibilitatea unui server dat, etc.

Această reformulare constă în definirea scării de valori sub forma unei „clasificări”.

Această formulare complementară constă în:

- Identificarea bunurilor care trebuie clasificate (informații, componentele sistemului informațional, aparate, etc.).
- Calificarea fiecărui bun ca o funcție a:
  - Modulii în care ar putea produce o defecțiune identificată
  - Gravității care rezultă.

Clasificarea sau estimarea informației și a bunurilor ajutătoare țintește să producă „etichete” care pot fi puse pe fiecare bun astfel încât persoanele care folosesc bunul să fie informate de importanța acestuia în securitate.

### 3.1 Identificarea elementelor care vor fi clasificate

Toate bunurile ar putea fi clasificate individual, fie că sunt informaționale sau elemente ajutătoare (precum site, elemente de procesare, sau rețea și comunicare).

În practică, este mai eficient să se grupeze informațiile, obiectele, sau bunurile care au roluri asemănătoare, și care necesită același tip și nivel de protecție. Deci, o aplicație și uneltele sale asociate, un set de tabele cu baze de date, etc., vor fi deseori grupate împreună din motive de clasificare.

***Nu toate obiectele care pot fi identificate într-o entitate ar trebui clasificate individual. Acestea ar trebui grupate. Aceste grupuri de informații și bunuri sunt cele care vor fi clasificate.***

Oricum, este practic și eficient să se facă distincția între:

- Elementele și bunurile care sunt legate în mod deosebit de procese sau domenii de activitate date, pe de o parte;
- Elemente de infrastructură și servicii comune, folosite de diferite domenii de activitate, pe de altă parte.

#### 3.1.1 Identificarea elementelor legate de procesele de afaceri

Pentru acele elemente și bunuri care sunt legate de procesele de afaceri sau domenii de activitate, este recomandat să se înceapă cu o listă a proceselor sau activităților (sau aplicațiilor IT). Acestea ar trebui unite în grupuri omogene, după cum s-a explicat mai sus. Pentru fiecare proces, aplicație sau domeniu de activitate, ar trebui identificate bunurile care trebuie clasificate.

De obicei, bunurile primare vor fi:

- Aplicații și proceduri (ap), ex: sursa și codul obiectului pentru procese IT. Pentru procesele care nu țin de IT, acest lucru ar necesita o descriere documentată a procedurilor;
- Date ale aplicațiilor sau baze de date (da);
- Date care sunt transmise sau schimbate între aplicații (tm);
- Fișiere desktop care sunt asociate cu procesul sau domeniul aplicației (fb);
- Listări și imprimări generate de aplicație (li);
- Documente și arhive ale personalului păstrate de persoane implicate în proces (ec);
- Poșta (electronică sau de alt tip) legată de procesul aplicației (cf);

Diferitele componente ajutătoare ale arhitecturii IT sunt identificate pentru a indica dacă acestea sunt implicate în fiecare proces sau domeniu aplicației. Aceste componente ar putea fi:

- Servere de aplicație (ASA);
- Servere desktop (ASB);
- Rețelele folosite (fie cu largă acoperire (WAN), locale(LAN), publice (PUB));
- Orice echipament specific folosit (AED);
- PC-uri portabile și orice alt echipament mobil (APM);

Tabelul completat va arăta oarecum ca partea superioară a „Proceselor de afaceri” din tabelul T1 de mai jos<sup>3</sup>:

---

<sup>3</sup> Este posibil să se ia în considerare alte componente ajutătoare (spațiile utile, locațiile...) în coloane adiționale

Tabelul T1 (Exemplu)	Tipuri de servicii	CLASIFICARE																	INFRASTRUCTURĂ							
		Aplicație și/sau proceduri			Date ale aplicației (baze de date)			Date ale aplicației în Mesaje tranzit			Fișiere desktop asociate			Lista	Document sau arhive scrise de mână		email sau poștă fax			Indicație (printr-un 1 sau un nume) că aplicația, procesul sau domeniul aplicației, necesită disponibilitatea bunurilor citate (servere, rețea, echipament specializat, dispozitive mobile sau portabile, etc.)						
		A	I	C	A	I	C	A	I	C	A	I	C	C	A	C	A	I	C	Apli Serv	desk top serv.	LAN	WAN	PD N	Echip. spec	Dispozitive mobile
Numele coloanei pentru Clasificare ~>		Aap	Iap	Cap	AAa	IAa	CAa	Atm	Itm	Ctm	Afb	Ifb	Cfb	Cli	Aec	Cec	Acf	Icf	Ccf	ASA	ASB	ARL	ARE	ARP	AED	APM
<i>Procese de afaceri</i>																										
Procesul 1 : HR		2	3	1	2	3	2	2	3	2	1	1	3	2	2	1	1	1	2	1						
Procesul 2 : Managementul vânzărilor		2	2	4	2	2	4	2	2	4	1	3	3		1	3	3	2	4	1		RLC	1			1
Procesul 3 : Planificarea strategică											2	2	3		1	3										
Procesul 4 : Domeniul financiar și contabil		2	2	3	2	2	3	2	2	3				1						1		1				
Procesul 5:		2	3	1	2	3	1	2	3	1	2	3	1								1	1				
Procesul 6 : CAD/CAM		3	3	3	3	3	3	3	3	3	3	3	3								Ulyse		1			1
Procesul 7 : site web comercial		3	3	1	3	3	1	3	3	1	1	1	1							1		1	1	Internet		1
.../...																										
Procesul N		2	2	1	2	2	1	2	2	1	2	2	1						1		1	1				
<i>Servicii comune</i>																										
e-mail		MSG	3	3	1	3	2	1	2	2										1		1	Wa n			
Serviciul poștal		COU		3													3	2	1							
Arhivarea fișierelor IT		ARI	3	3	1	3	3	1	1	1	2	1	1													
Arhivele documentelor		ARD	3	3	1	3	3	1	1	1	2	1	1							1		1				
Adminstrarea sistemului		ADM	2	3	1	2	3	1	1	3	1	1	1	3	1	3					1	1				
Ajutorul & sprijinul utilizatorului		HLP	3	1	1	3	1	1	1	1	1	1	1							1		1			1	

**Tabelul T1. Clasificarea bunurilor și componentele ajutătoare.**

Merită menționat faptul că, în acest tabel componentele de infrastructură (bunurile ajutoare) sunt menționate pentru fiecare proces care le folosește. Clasificarea se aplică doar componentelor specifice proceselor entității: aplicații, proceduri și diferite tipuri de date sau informații. Clasificarea componentelor comune sau dedicate infrastructurii folosite pentru crearea, procesarea, transmiterea sau consultarea informațiilor pot fi deduse logic din clasificarea elementelor funcționale dependente.

Ar trebui reținut și faptul că componentele de infrastructură menționate în tabel pot fi dedicate (precum serverele de aplicație) sau comune (precum rețeaua cu acoperire largă). Acest tabel este important deoarece scoate la iveală, în timpul clasificării, constrângerile impuse de mizele de securitate ale fiecărei activități asupra IT și arhitecturii comunicării. Acest lucru, în sine, poate conduce la necesitatea de a defini sub-domenii pentru anumite activități (sau sub-procese), pentru a scoate la iveală bunuri de infrastructură specifice (de exemplu, pentru a evidenția activitățile care folosesc PC-uri portabile).

Componentele de infrastructură care sunt folosite de către diferitele procese ar trebui identificate, aplicație cu aplicație:

- Fie prin simpla observație că sunt folosite de către aplicație, de către un 1 (celulă altfel goală);
- Sau prin specificarea numelui lor: nume (sub) rețea, nume server, etc. dacă este necesar să se diferențieze elementele de aceeași natură.

### **3.1.2 Identificarea elementelor legate de serviciile comune**

Este posibil întotdeauna ca anumite servicii comune să nu fi fost identificate ca elemente critice în timpul analizei proceselor de afacere. Totuși, ele pot fi critice (într-o măsură mai mică sau mai mare) pentru întreprindere sau organizație ca întreg.

Acesta ar fi cazul când, de exemplu, ele ar putea influența planificarea sau strategia de dezvoltare IT, sau când ele ar putea avea un impact asupra imaginii profesionale a organizației sau a serviciilor sale ajutoare, fie pe plan intern sau extern.

Mai jos este o listă non-exhaustivă cu ce se consideră în general ca fiind servicii comune:

- Poșta electronică (MSG);
- Serviciile poștale (COU);
- Arhivarea fișierelor IT (ARI);
- Arhivarea documentelor (ARD);
- Administrarea sistemului pentru IT și telecomunicații (ADM);
- Servicii de ajutorare a utilizatorului (HLP);
- Etc.

Aceste servicii comune ar trebui identificate și clasificate, precum cele pentru procesele de afacere menționate mai sus. Ele sunt incluse în partea de jos a tabelului T1.

### **3.1.3 Identificarea infrastructurii ajutoare comune care trebuie clasificată**

În ceea ce privește bunurile ajutoare dedicate (cele folosite de către procesele de aplicație pentru a crea, procesa, transmite și consulta informația), clasificarea lor poate fi dedusă cu ușurință din cea a datelor și informațiilor. Astfel, un server care găzduiește o aplicație (date sau program) va avea același nivel de clasificare pentru un criteriu dat (disponibilitate, de exemplu) precum aplicația care este găzduită.

În ceea ce privește bunurile comune, nivelul clasificării, pentru fiecare criteriu (A, I, C), este nivelul maxim indus din toate procesele de aplicație dependente.

Anumite elemente ale infrastructurii generale ar trebui totuși identificate separat. Acestea sunt cele ale căror clasificare nu va depinde doar de clasificarea acelor procese care le folosesc.

Acestea ar fi bunuri de infrastructură ale căror modificare ar avea o influență asupra IT-ului și a comportamentului utilizatorului sau a imaginii de corporație a organizației și a serviciilor sale ajutoare (pe plan intern sau extern). Astfel de bunuri de infrastructură merită o evaluare complementară a nivelurilor lor critice. Acestea ar fi în mod tipic:

- rețea locală (RL);

- rețea cu acoperire largă (RE);
- rețea de telefonie (RT);
- servere de aplicație (SV) și comune (SS);
- periferice (inclusiv, de exemplu, serviciile de imprimare, și serverele lor de printare) (PF);
- portaluri către servicii externe (ex. Internet) (PA);
- spațiul util (ET).

Aceste bunuri de infrastructură ar trebui examinate în mod specific, și apoi pot fi documentate într-un nou tabel (T2), cu coloane specifice. Un exemplu este arătat mai jos:

Tabelul T2 (Exemplu)	FUNCTIE Opțional (descriere)	Sub- clasa infra- struct	CLASSIFICATION								
			cablare & echip.			Fișiere de configurare			Biblioteca programul ui sistemului		
Componente de infrastructură			A	I	A	I	C	A	I	C	
Numele coloanei pentru formulele de clasificare		SCA	Aeq	Ieq	Afc	Ifc	Cfc	Alp	Ilp	Clp	
LAN-uri		RL	2	3	3	3	3	1	2	1	
WAN-uri		RE	2	2	3	3	2	1	2	1	
Rețea de telefonie		RT	3	2	2	3	3	1	2	1	
Servere de aplicație & servere de date		SV	2	2	3	2	1	1	2	1	
Servere IT sau de serviciu de rețea (DNS, LDAP, server de autentificare, etc.)		SS	2	2	2	3	1	1	3	1	
Periferice		PF	1	1				1	2	1	
Portaluri de acces		PA	2	2	1	2	1	1	2	1	
Mediu global de lucru		ET	2	1							

**Tabelul 2: Clasificarea infrastructurii comune**

## 3.2 Criteriile de clasificare

Pierderea disponibilității, integrității, sau a confidențialității<sup>4</sup> unui bun poate avea consecințe operaționale și de afaceri care trebuie evaluate. Tabelele de mai sus trebuie completate cu o valoare (de la 1 la 4) pentru fiecare tip de bun și criteriu.

Consecințele pierderii disponibilității, integrității, sau a confidențialității pentru datele aplicației sunt afișate în coloanele Ada, Ida, Cda, ale tabelului T1.

Același lucru se aplică pentru datele office asociate (Afb, Ifb, Cfb);

Pentru printuri, de obicei doar confidențialitatea este luată în discuție (Cli). Totuși, pentru documentele scrise și arhive, disponibilitatea poate fi adăugată la confidențialitate (Aec, Cec).

Pentru aplicații și programe, principala preocupare o reprezintă pierderea disponibilității sau a integrității (Aap, Iap). Totuși, confidențialitatea (Cap) poate reprezenta și ea o preocupare pentru anumite aplicații care oferă avantaj competitiv pentru entitate.

Poșta, fie ea electronică sau nu, este rareori considerată la nivelul domeniului aplicației, cu excepția confidențialității. Disponibilitatea serverului de poștă este acoperită în altă parte, ca parte a serviciilor comune (rândul MSG +coloana ASA din Tabelul T1).

Pentru cablare și componentele infrastructurii, fișierele de configurare și bibliotecile de programe, principala preocupare o reprezintă pierderea disponibilității sau a integrității, cu excepția cazurilor specifice (vezi Tabelul T2).

Pentru fișierele de configurare, se aplică toate criteriile.

## 3.3 Procesul clasificării

### 3.3.1 Clasificarea bunurilor care sprijină procesele de afaceri

Pentru fiecare grupă de bunuri care sprijină procesele de afaceri sau un domeniu de activitate, va fi

<sup>4</sup> Este posibil să se definească cauzele adiționale ale defecțiunii, și astfel criteriile de clasificare. Cel de-al treilea este de obicei „dovada” sau „valoarea dovezii”.

realizată o analiză pentru a determina dacă o pierdere a confidențialității ar putea conduce la una sau mai multe posibile defecțiuni, și, dacă acesta este cazul, la ce nivel al defecțiunii. Dacă din pierderea confidențialității pentru un bun ar putea rezulta mai multe defecțiuni potențiale, este reținut cel mai înalt nivel al acestora (pe o scară de la 1 la 4) pentru criteriul de confidențialitate.

Același lucru este valabil pentru alte criterii (disponibilitatea și integritatea) care rezultă, pentru fiecare grupă de bunuri identificată, într-o valoare a clasificării pentru fiecare criteriu (Disponibilitate, Integritate Confidențialitate).

Scopul clasificării este astfel de a defini, pentru grupurile de bunuri identificate, „etichete” care vor arăta nivelurile consecințelor unei pierderi a disponibilității, integrității sau confidențialității pentru fiecare clasă de bunuri.

### **3.3.2 Clasificarea elementelor legate de serviciile comune**

Aceeași abordare este valabilă și pentru serviciile comune. Merită totuși observat faptul că în acest caz noțiunea disponibilității datelor aplicației reprezintă mai degrabă o disciplină globală care țintește să ofere păstrarea completă a datelor (de exemplu, întreaga bază de mesaje a serviciului poștal), în timp ce în partea de activitate, este mai degrabă o chestiune de disponibilitatea în ceea ce privește timpul de răspuns necesar.

Pentru aceste servicii comune, poate fi necesar o reîntoarcere la abordarea analizei mizelor (precum și pentru scara de valori a defecțiunilor), pentru a evalua impactul unei schimbări a serviciilor.

### **3.3.3 Clasificarea elementelor de infrastructură globală**

De asemenea, pentru elementele de infrastructură globală, eforturile ar trebui concentrate asupra impactului total al schimbării elementelor. Impactul particular asupra afacerii a fost analizat de către scara de valori a defecțiunilor și în timpul creării tabelului T1.

În particular, ar trebui evaluat impactul indisponibilității fișierelor de configurare (Tableul T2), luând în considerare timpul care poate fi necesar pentru a reconfigura toate componentele implicate. Acest lucru ar putea fi necesar dacă există o pierdere generală a configurației sau a fișierelor cu parametri, oricare ar fi motivul pentru asta, ca parte a unui plan de rezervă/refacere, etc. Indisponibilitatea fiecărui fișier de configurare (la nivelul unei activități individuale) care este deja evaluat la nivelul procesului aplicației (care ar putea avea un impact mult mai mic).

## 4 Construirea tabelului impactului intrinsec

În timpul procesului MEHARI de analiză a riscului, este introdusă noțiunea de impact intrinsec al unui scenariu. Aceasta reprezintă evaluarea consecințelor producerii unui scenariu de risc independent de orice măsuri de securitate (Vezi documentul „*Concepte Generale și Mecanisme Principale MEHARI*”, precum și „*Ghidul Analizei Riscului*”).

Mai exact, baza de cunoștințe MEHARI se referă la un tabel al impactului intrinsec, care poate fi completat cu informații din tabelele de clasificare discutate mai devreme.

Un extras din acest tabel (arătat în Anexa 2) este dat mai jos:

<i>Tabelul Impactului Intrinsec</i>			
<b>Clasificarea datelor, informațiilor și componentelor infrastructurii</b>	A	I	C
<b>Datele și informațiile</b>			
D01 Fișiere cu date sau baze de date ale aplicațiilor			
D07 Poșta și faxurile			
.../...			
<b>Infrastructura IT și cea telecom</b>			
R02 Echipament și legături LAN			
S01 Mainframe-uri, servere de informații,.....			

Procesul pentru completarea tabelului impactului intrinsec beneficiază de tabelele de clasificare a bunurilor (T1 și T2) care au fost definite și descrise în secțiunea anterioară.

În total, procesul constă, pentru fiecare rând al tabelului impactului intrinsec, și pentru fiecare criteriu de clasificare (A, I sau C) în:

- selectarea elementelor relevante din tabelele de clasificare;
- identificarea, pentru fiecare element selectat, a nivelului maxim de clasificare, și copierea acestuia în tabelul impactului intrinsec;

Elementele selectate sunt arătate în tabelul T3 de mai jos, unde fiecare câmp arată:

- În coloanele A, I, sau C, cea mai mare valoare găsită în coloane identice ale tabelelor T1 și T2;
- În coloana Condiție, criteriul pentru selectarea rândurilor din tabelele T1 și T2 astfel încât să fie extrase din fiecare tabel doar acele elemente care sunt atât în rândurile cât și în coloanele selectate.

## Formulele Tabelului Impactului Intrinsec

Formulele Tabelului Impactului Intrinsec						
Clasificarea datelor, informațiilor și a componentelor infrastructurii					Regulă	
Date și informații	A	I	C	Condiție		
D01	Fișiere de date sau date de baze ale aplicațiilor		T1 : coloana Ida	T1 : coloana Cda		1
D02	Fișiere desktop depozitate pe server de acces comun	T1 : coloana Afb	T1 : coloana lfb	T1 : coloana Cfb	Rânduri precum ASB # ""	2
D03	Fișiere desktop depozitate pe o stație de lucru personală	T1 : coloana Afb	T1 : coloana: lfb	T1 : coloana Cfb	Rânduri precum ASB = ""	2
D04	Informații scrise de mână sau printate deținute de către utilizatori, arhive personale	T1 : coloana Aec		T1 : coloana Cec		1
D05	Listări sau printări cu aplicații IT			T1 : coloana Cli		1
D06	Mesaaje trimise, date în tranzit	T1 : coloana Atm	T1 : coloana ltm	T1 : coloana Ctm		1
D07	Postă și Faxuri	T1 : coloana Acf	T1 : coloana lcf	T1 : coloana Ccf		1
D08	Arhive istorice, arhive cu valoare de dovadă	T1 : coloana Aec			Rândurile Typ ARI și ARD	3
DU	Date și informații publicate pe site-uri web publice	T1 : coloana AAa	T1 : coloana Ida	T1 : coloana Cda	Rânduri precum ARP # ""	2
<i>Infrastructura IT și a comunicațiilor</i>						
R01	Link-uri și echipament WAN (sisteme de rețea și software-ul lor)	T1 : coloana AAa T2 : coloana Aeq	T1 : coloanele Cda, Ida și lap T2 : coloana leq		T1 Rânduri precum ARE # "" T2 Rândul: SCA=RE	2 și 4
R02	Link-uri și echipament LAN (sisteme de rețea și software-ul lor)	T1 : coloana AAa T2 : coloana Aeq	T1 : coloana Cda, Ida și lap T2 : coloana leq		T1 Rânduri precum ARL # "" T2 Rândul: SCA = RL	2 și 4
R03	Date de configurare WAN	T2 : coloana Afc	T2 : coloana lfc	T2 : coloana Cfc	T2 Rândul: SCA = RE	4
R04	Date de configurare LAN	T2 : coloana Afc	T2 : coloana lfc	T2 : coloana Cfc	T2 Rândul: SCA = RE	4
S01	Mainframe-uri, servere de aplicații, și periferice centrale dedicate, servere de fișiere comune	T1 : coloana AAa T2 : coloana Aeq	T1 : coloana Cda, Ida and lap T2 : coloana leq		T1 Rânduri precum ASA # "" T2 Rândul: SCA = SV sau SS	2 și 4
S02	Fișiere de sistem și de configurare a serverului	T2 : coloana Afc	T2 : coloana lfc	T2 : coloana Cfc	T2 Rândul: SCA = SV	4
S03	Echipament pentru terminal disponibil utilizatorilor (PC-uri, periferice, dispozitive speciale)	T1 : coloana AAa T2 : coloana			T1 Rânduri precum AED# "" T2 Rândul: SCA = PF	2 și 4
A01		T1 : coloana Aap	T1 : coloana lap	T1 : coloana Cap		1
<i>Infrastructura generală</i>						
E01	Mediul de lucru al utilizatorului	T1 : coloanele Afb și Aec T2 : coloana Aeq			Toate rândurile T1 T2 Rândul: SCA = ET	1 și 4
E02	Echipament de telecomunicații oral sau analogic	T2 : coloana Aeq	T2 : coloana leq		T2 Rândul: SCA = RT	4
I01	Întreaga instalație a camerei IT sau de telecomunicații	T1 : coloanele Aap și AAa T2 : coloana Aeq				1

Ultima parte a Tabelului T3 corespunde impacturilor intrinseci care nu depind de clasificarea unui bun. De fapt, necesită evaluarea impactului intrinsec a unor tipuri de scenarii mai deosebite. În practică, acestea vor privi indisponibilitatea personalului sau neaderența la legi sau directive.

Această parte ar trebui să fie subiectul unei analize specifice care să ia în calcul consecințele posibile ale unui scenariu de risc și impactul intrinsec direct evaluat, în mod independent de orice clasificare.

## 5 Sfaturi practice

### 5.1 Puncte importante care trebuie luate în considerare în crearea scării de valori

#### 5.1.1 Concentrați-vă asupra aspectelor celor mai critice

*Este important să vă concentrați asupra principalelor defecțiuni, și nu să încercați să luați în considerare fiecare scenariu de risc posibil.*

Primul scop al securității, indiferent de abordarea folosită, este cel de a evita producerea problemelor grave sau foarte grave. Acestea reprezintă riscuri care trebuie, de aceea, să fie identificate și examinate.

Acesta este motivul pentru care este foarte recomandat ca managementul de top și cei responsabili pentru o activitate dată să fie implicați direct în procesul de evaluare. Nu ar trebui delegat niciodată unui delegat.

În practică, pentru fiecare activitate, cel mai bine este să se concentreze un număr mic de defecțiuni critice (de obicei între 3 și 8).

#### 5.1.2 Excluderea controalelor existente

În al doilea rând, dar la fel de important, defecțiunile care par imposibile la prima vedere nu ar trebui ignorate. Este întâlnit prea des cazul în care managementul alungă din minte producerea potențială a unui accident care ar putea pierde toate datele importante, prin pretextul că datele sunt computerizate și deci arhivate de către sistemul IT. *Defecțiunile, și gravitatea lor, ar trebui identificate și evaluate fără a lua în considerare controalele de securitate existente, chiar dacă acele măsuri sunt implementate solid.* Altfel, acest lucru ar putea conduce la concluzia că nimic nu este supus riscului, și că controalele de securitate nu sunt necesare, și deci pot fi scoase din calcul.

*De asemenea, natura mai mult sau mai puțin probabilă a unui eveniment care conduce la defecțiune nu ar trebui luată în considerare în timpul acestei faze a abordării.*

#### 5.1.3 Consistența defecțiunilor de diferite tipuri

Un alt punct important în determinarea criteriilor și a pragurilor critice este de a menține o consistență între diferite tipuri de defecțiuni care au nivele de gravitate echivalente.

Cu acest scop în minte, este recomandat să se definească axe strategice care pot fi folosite ca referință pentru a asigura consistența nivelelor de gravitate pentru diferite defecțiuni.

Una din axele de evaluare poate fi financiară. Astfel, echivalentele financiare ar fi căutate pentru fiecare tip de defecțiune. De asemenea, o axă de „serviciu pentru public” ar reprezenta referința pentru compararea impactului individual, mărimea populației etc.

#### 5.1.4 Aspecte strategice și de luare a deciziilor ale scării de valori

Deseori, gravitatea unor defecțiuni nu poate fi evaluată. Acest lucru ar putea fi din cauză că consecințele indirecte sunt greu de identificat, sau din cauză că este prea greu să evalueze serios eficiența acțiunilor care ar putea fi realizate în situația dată.

*În unele situații, gravitatea defecțiunii poate fi rezultatul unei simple decizii.*

*Nu există o evaluare formală ci o decizie strategică pentru întreprindere sau organizație care spune că o defecțiune dată ar trebui considerată ca fiind gravă, foarte gravă, sau vitală.*

## 5.2 Puncte importante în timpul clasificării

Mai întâi, este important să se grupeze corespunzător bunurile cu scopurile similare pentru a nu trebui să se analizeze cantități mari de obiecte.

***Un bun punct de plecare este gruparea aplicațiilor în domenii.***

În al doilea rând, este recomandat să se planifice un pas de consolidare și validare la nivelul fiecărei entități, precum și pentru scara de valori.

## 5.3 Limite pentru clasificare

În mod clar, procesul care a fost descris, fie el creația scării de valori sau clasificarea, se pliază unei entități cu independență decizională și propriile sale scopuri. Aceasta ar putea fi afiliată (național sau regional) unui grup de corporații, sau unei unități de afaceri, sau unui serviciu operațional sau funcțional cu o responsabilitate bine definită.

Scara de valori a defecțiunilor și clasificarea informațiilor și a bunurilor care sunt definite pentru o entitate sunt evident valabile pentru acea entitate. Totuși, care este valoarea lor în afara acelei entități?

***Prin definiție, clasificarea definită pentru o entitate reprezintă mijlocul de a împărți și comunica sensibilitatea unui bun care aparține acelei entități. Această clasificare este valabilă în întreprindere.***

De fapt, aceasta este o regulă a schimbului de elemente (mai ales informații) între entități. Dacă o entitate A (o agenție mică, de exemplu) consideră că confidențialitatea informației este vitală, și o clasifică ca atare, nu este posibil ca entitatea B (sediul central de exemplu) să regândească clasificarea și să decidă că informația nu este sensibilă. Dacă s-ar permite ca lucrul din urmă să aibă loc, atunci entitatea A ar trebui să decidă să nu transmită informații entității B.

Această noțiune de limite ale valabilității pentru clasificare este deosebit de importantă în managementul securității pe baza unei reguli stabilite numite „Cadrul de referință în securitate”.

În exemplul de mai sus, precauțiile sau controalele de securitate care vor fi aplicate ca funcție a clasificării sunt cunoscute. Ar fi stupid ca o entitate să protejeze informațiile aliniate la un nivel al clasificării și ca alte entități să aplice alte reguli de protejare pentru aceeași informație. În mod deosebit, ar fi periculos pentru o altă entitate să decidă de una singură că informația nu trebuie protejată la nivelul hotărât de o altă entitate.

## 5.4 Planuri de acțiune

Aici, vom acoperi construirea planurilor de securitate direct din analiza mizelor.

Totuși, merită observat faptul că interviurile individuale care contribuie la crearea scării de valori, împreună cu o ședință a managementului, în care sunt discutate cele mai grave defecțiuni, ar trebui să dea naștere la planuri de acțiune urgente. Orice manager ar fi frustrat să petreacă timp cu o analiză și identificare a vulnerabilităților, doar ca să afle că nu reiese nimic de aici.

***Ar trebui, deci să fie întocmit un plan de acțiune pentru acțiunile cele mai urgente. Acest lucru ar trebui poate discutat și aprobat într-o ședință a managementului, imediat după ce analiza mizelor este terminată.***

# Anexa 1: Exemplu al unei scări de valori (întreprindere industrială)

## 1. Managementul finanțelor și al bugetului

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Pierdere financiară</i>	Pierdere < 1 M€	Pierdere între 1 M€ și 10 M€	Pierdere între 10 și 100 M€	Pierdere > 100 M€
<i>Fraudă sau delapidare</i>	Fraudă sau delapidare în achiziționarea și plata corespondentă sau în managementul livrării.			
<i>Incapacitatea de a factura bunurile livrate</i>	Incapacitatea globală de a factura pentru o perioadă de mai puțin de o săptămână	Incapacitatea globală de a factura pentru o perioadă cuprinsă între o săptămână și o lună. Pierderea informațiilor privind livrările efectuate într-o zi.	Incapacitatea globală de a factura pentru o perioadă mai mare de o lună. Pierdea completă a dovezii livrării pentru o întreagă săptămână.	
<i>Defecțiunea procesului de memento al clienților</i>	Indisponibilitatea temporară a sistemului de memento.	Indisponibilitatea pe termen lung a sistemului de memento.		

## 2. Strategie – Indicații generale – Management și urmărire

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Dezvăluirea datelor sau a informațiilor privind planurile pe termen lung sau cele strategice.</i>		Dezvăluirea planurilor pe termen lung ale unui afiliat. Dezvăluirea bugetului Dezvăluirea rapoartelor lunare	Dezvăluirea informațiilor privind evoluția strategică Dezvăluirea planurilor pe termen lung consolidate ale întreprinderii	
<i>Indisponibilitatea analizei rezultatelor sau a sistemului intern de raportare</i>	Indisponibilitatea procesului de raportare lunară	Incapacitatea de a face rapoarte sau analiza rezultatelor pentru mai mult de 2 luni		
<i>Coruperea datelor de raportare și a rapoartelor lunare</i>	Coruperea datelor elementare sau informații mărite pe baza unor date elementare.			

## 3. Dezvoltarea afacerii – managementul clientului

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Dezvăluirea informațiilor privind operațiunile de dezvoltare a afacerii</i>	Dezvăluirea notelor și sumarelor directorilor privind dezvoltarea afacerii			
<i>Dezvăluirea condițiilor financiare</i>	<i>Dezvăluirea condițiilor financiare specifice unui anumit client</i>	<i>Dezvăluirea documentelor strategiei de fixare a prețului</i>	<i>Dezvăluirea condițiilor financiare pentru toți clienții.</i>	
<i>Dezvăluirea informațiilor despre client</i>	<i>Dezvăluirea unor elemente ale bazei de informații a clienților</i>	<i>Dezvăluirea informațiilor despre toți clienții</i>		

#### 4. Cercetare și dezvoltare

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Dezvăluirea informațiilor tehnice</i>	Dezvăluirea modelelor de simulare	Dezvăluirea buletinelor tehnice curente Dezvăluirea informațiilor despre specificațiile sau procedurile interne și despre evoluția curentă	Dezvăluirea buletinelor tehnice în cazuri excepționale Dezvăluirea informațiilor asupra impactului evoluției tehnice, rezultând în închiderea unităților.	
<i>Încălcarea acordurilor de confidențialitate</i>		Încălcarea acordurilor de confidențialitate cu partenerii	Încălcarea acordurilor de confidențialitate cu furnizorii cheie de tehnologie	
<i>Pierderea expertizei</i>			Pierderea arhivelor a memorandumurilor și a buletinelor tehnice privind dezvoltarea tehnică.	

#### 5. Managementul procesului industrial – Proiecte pentru evoluție - Întreținere

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Pierderea arhivelor de documente a proiectului de evoluție Pierderea documentației tehnice pentru echipamentul existent</i>	Pierderea arhivelor proiectului pe durata de viață a proiectului. Pierderea copiilor în original a planurilor echipamentului care au fost aprobate de către autoritățile competente.	Pierderea totală a arhivelor pe termen lung privind echipamentul și modificările făcute la acesta.		
<i>Defecțiuni care conduce la folosirea planurilor de instalare incorecte în timpul evoluției și actualizărilor</i>			Erori în, sau schimbări la planurile de instalare existente, sau defecțiunea managementului de schimbare.	
<i>Dezvăluirea informațiilor tehnice</i>		Dezvăluirea temelor de muncă și a programului de cercetare a pre-proiectului	Dezvăluirea tuturor dosarelor pre-proiectului (inclusiv poziționarea strategică a proiectului)	
<i>Indisponibilitatea uneltelor de management al proiectului</i>	Indisponibilitatea uneltelor interne de planificare Indisponibilitatea uneltelor de management al ordinii pentru mai puțin de o săptămână	Indisponibilitatea uneltelor de management al ordinii pentru mai mult de o săptămână		
<i>Defecțiuni în managementul de întreținere</i>	Pierderea bazei de date a acțiunii de întreținere planificate	Indisponibilitatea uneltelor de management al întreținerii pentru mai puțin de o lună Pierderea datelor tehnice și istorice necesare pentru planificarea întreținerii	Indisponibilitatea uneltelor de management al întreținerii pentru mai mult de o lună Schimbări ale parametrilor uneltelor de management al întreținerii	

## 6. Producție și livrare - Logistică

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Producția oprită (nici un sistem nu este disponibil, pierderea unui element critic)</i>	Nici un fel de producție pentru mai mult de o săptămână	Nici un fel de producție pentru o perioadă între 1 săptămână și 1 lună.  Pierderea unui element critic, conducând la pierderea producției pentru mai puțin de 1 lună.	Nici un fel de producție între 1 și 3 luni.  Pierderea unui element critic, conducând la pierderea producției pentru o perioadă între 1 și 3 luni	Producția oprită pentru mai mult de 3 luni.  Pierderea unui element critic, conducând la pierderea producției pentru mai mult de 3 luni.
<i>Unelte de management al producției indisponibile</i>	Uneltele de management al producției indisponibile pentru mai puțin de o săptămână	Uneltele de management al producției indisponibile pentru o perioadă cuprinsă între o săptămână și o lună	Uneltele de management al producției indisponibile pentru mai mult de o lună	
<i>Coruperea uneltelor de management al producției sau falsificarea parametrilor de management</i>			Modificarea managementului de producție conducând la neconformitatea produselor	Modificarea managementului de producție conducând la accidente sau la deteriorarea uneltelor de producție
<i>Incapacitatea de a asigura logistica pentru livrarea produselor</i>	Incapacitatea de a asigura livrările critice pentru mai puțin de o săptămână	Incapacitatea de a asigura livrările critice pentru mai mult de o săptămână		

## 7. Relațiile cu părțile terțe (altele decât comerciale)

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Dezvăluirea informațiilor asupra rezultatelor corporației</i>		Publicarea prematură a rezultatelor unui afiliat	Publicarea prematură a conturilor consolidate	
<i>Defecțiune în procesul pentru consolidarea conturilor anuale</i>	Întârziere în publicarea conturilor de mai puțin de 2 săptămâni	Întârziere în publicarea conturilor de mai mult de 2 săptămâni	Pierderea totală a tuturor elementelor financiare necesare pentru producerea conturilor anuale	
<i>Dezvăluirea notelor sau a memoriilor privind riscurile, operațiunile sau mecanismele fiscale</i>	Dezvăluirea notelor sau a memoriilor privind riscurile, operațiunile sau mecanismele fiscale în funcție de conținutul notei sau al memoriului			
<i>Pierderea elementelor istorice care justifică o operațiune fiscală</i>	Pierderea elementelor istorice care justifică o operațiune fiscală			
<i>Plata târzie a taxelor și impozitelor</i>		Indisponibilitatea uneltelor de calcul a plății taxelor		
<i>Pierderea documentelor oficiale sau a arhivelor</i>		Pierderea autorizațiilor oficiale pentru a opera	Pierderea documentelor oficiale sau a arhivelor care sunt cerute din punct de vedere legal de către procedurile administrative (taxe, export)	

## 8. Managementul reclamațiilor – aspecte legale și penale

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Dezvăluirea probelor sau argumentelor legate de o reclamație.</i>	Dezvăluirea informațiilor privind o reclamație în curs.	Dezvăluirea informațiilor privind o reclamație excepțională.		
<i>Dezvăluirea a părți dintr-o expunere penală privind personalul</i>		Dezvăluirea a părți dintr-o expunere penală curentă	Dezvăluirea a părți dintr-o expunere penală în circumstanțe excepționale	
<i>Pierderea sau dispariția originalelor unor documente</i>	Pierderea sau dispariția contractelor originale	Pierderea sau dispariția originalelor unor acorduri specifice, declarații de intenție, etc.		

## 9. Managementul HR

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Dezvăluirea informațiilor personale</i>	Dezvăluirea salariului unui angajat	Dezvăluirea salariilor întreg personalului	Dezvăluirea repetată a salariilor întreg personalului	
<i>Întârzieri la plata salariilor</i>	Întârziere < 2 zile	Întârzieri între 2 și 15 zile	Întârzieri > 15 zile	
<i>Distrugerea datelor de bază privind plata salariilor (calcul și parametri)</i>	Ștergerea datelor recente (nu mai vechi de o lună)	Ștergerea datelor pentru întregul an	Ștergerea tuturor datelor, inclusiv a datelor istorice	

## 10. Sistemul informațional

<i>Defecțiune</i>	<i>Nivelul 1 Nesemnificativ</i>	<i>Nivelul 2 Grav</i>	<i>Nivelul 3 Foarte grav</i>	<i>Nivelul 4 Vital</i>
<i>Indisponibilitatea rețelei și a serverelor (date comune și personale)</i>	Indisponibilitatea pentru mai puțin de o lună	Indisponibilitatea pentru mai mult de o lună		
<i>Indisponibilitatea sistemului de e-mail</i>	Indisponibilitatea sistemului de e-mail			
<i>Indisponibilitatea rețelei de telefonie</i>	Indisponibilitatea rețelei de telefonie			
<i>Pierderea arhivelor</i>		Pierderea serverelor de date, sau a arhivelor de e-mail		
<i>Crearea ilicită a drepturilor de administrare asupra sistemului</i>			Coruperea tabelului drepturilor de acces și crearea drepturilor de administrare	
<i>Dezvăluirea informațiilor despre sistem sau arhitectură</i>			Dezvăluirea rapoartelor directorilor sau a informațiilor detaliate privind securitatea sistemului și slăbiciuni necorectate.	

## Anexa 2: Tabelul Impactului Intrinsec

Tabelul Impactului Intrinsec

Nivelul clasificării datelor, informațiilor și al componentelor de infrastructură		A	I	C
<b>Date și informații</b>				
D01	Fișiere de date sau baze de date accesate de aplicații			
D02	Fișierele și datele office comune			
D03	Fișiere office personale (pe PC, etc.)			
D04	Informații și date scrise sau printate păstrate de utilizatori și arhive personale			
D05	Listări sau documente printate			
D06	Mesaje trimise, screen view-uri, etc. (date parțiale)			
D07	Poșta și faxuri			
D08	Documente sau arhive patrimoniale folosite ca dovezi			
D09	Date și informații publicate pe site-uri publice sau interne			
<b>Infrastructură : telecomunicații și sisteme</b>				
R01	Echipament și cablaj pentru rețeaua cu largă acoperire (sisteme de rețea și software asociat)			
R02	Echipament și cablaj pentru rețeaua locală (sisteme de rețea și software asociat)			
R03	Date de configurare pentru WAN			
R04	Date de configurare pentru LAN			
S01	Sisteme principale, servere care găzduiesc aplicații și echipamentele lor periferice, servere de fișiere comune			
S02	Fișiere de configurare legate de sistemele și serverele principale			
S03	Stații de lucru și terminale (PC, imprimante locale periferice, interfețe specifice, etc.)			
A01	Software, package sau middleware pentru aplicații (cod executabil)			
A02	Cod sursă			
A03	Fișiere de configurare legate de aplicații			
A04	Aplicații și software al utilizatorului sau clientului			
<b>Infrastructura generală</b>				
E01	Spațiul de lucru și mediul utilizatorului			
E02	Echipamente folosite pentru schimburile orale (telefon, etc.)			
I01	Totalitatea camerei computerelor și premise telecom			
<b>Impacturi intrinseci (obiecte globale sau nelegate de un anumit obiect)</b>				
<b>Indisponibilitatea personalului</b>				
P01	Echipe de specialiști (legat de afaceri)			
P02	Personalul pentru operațiuni IT			
<b>Neconformarea legală și reglementară</b>				
C01	Neconformarea la legi și reglementări privind protecția vieții private			
C02	Neconformarea la legi și reglementări privind controalele financiare			
C03	Neconformarea la legi și reglementări privind drepturile de proprietate intelectuală			
C04	Neconformarea la legi și reglementări privind protecția sistemului informațional			
C05	Neconformarea la legi și reglementări privind punerea în pericol a personalului și a siguranței publice și a mediului			