

MEHARI 2010

Analiza mizelor de securitate si ghidul de clasificare

Noiembrie 2010



Comisia Metodelor

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 75009 PARIS (France)

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr

Web : <http://www.clusif.asso.fr>

Mehari este marcă înregistrată a CLUSIF

MULȚUMIRI

Clusif ar dori să mulțumească în special lui Jean-Philippe Jouas pentru contribuția sa, lui Jean-Louis Roule pentru traducere cât și membrilor comisiei Metodelor care au participat la realizarea acestui document.

Traducerea în limba română a fost realizată de **Lazareanu Elena-Luiza** studenta a Facultății de Economie și Administrarea Afacerilor din cadrul Universității Alexandru Ioan Cuza din Iași.

Proiectul a fost coordonat de **dr. Valentin-Petru Măzăreanu**, cercetător postdoc și cadru didactic asociat în instituția mai sus menționată.

Contact:

www.managementul-riscurilor.ro

CUPRINS

1. Introducere	4
2. Scara de valori a defectiunilor	5
2.1. Identificarea principalelor activitati si obiectivele lor	6
2.1.1 Rezultatele prevazute	6
2.1.2 Abordare	6
2.2. Identificarea potentialelor defectiuni.....	6
2.2.1. Rezultatele prevazute	6
2.2.1.1. Potentiale defectiuni identificate la nivel functional.....	7
2.2.1.2. Potentiale defectiuni identificate la nivel tehnic	8
2.2.2 Abordare.....	9
2.3 Analiza mizelor de securitate: evaluarea gravității defectiunilor identificate	9
2.3.1 Scara gravității	9
2.3.2 Criteriile defectiunii și praguri de criticalitate: rezultate elementare	10
2.3.3 Abordare.....	11
2.4 Scara de valori a defectiunilor	11
3. Clasificarea informației și a bunurilor ajutătoare	12
3.1 Identificarea elementelor care vor fi clasificate	12
3.1.1 Identificarea elementelor legate de procesele de afaceri.....	13
3.1.2. Identificarea elementelor legate de politica de securitate a companiei	15
3.2 Criteriile de clasificare	15
3.3. Procesul de clasificare	15
3.3.1 Clasificarea bunurilor care sprijină procesele de afaceri.....	15
3.3.2. Clasificarea bunurilor la nivel corporativ	16
4. Construirea tabelului impactului intrinsec	17
5. Sfaturi practice	17
5.1 Puncte importante care trebuiesc luate în considerare în crearea scării de valori	17
5.1.1 Concentrați-vă asupra aspectelor celor mai critice	17
5.1.2 Excluderea controalelor existente	17
5.1.3 Consistența defectiunilor de diferite tipuri	18
5.1.4 Aspecte strategice și de luare a deciziilor ale scării de valori	18
5.2 Puncte importante în timpul clasificării.....	18
5.3 Limite pentru clasificare	18
5.4 Planuri de acțiune	19
Anexa 1: Exemplu al unei scări de valori (întreprindere industrială)	20
Anexa 2: Tabelul Impactului Intrinsec	28

1.Introducere

Analiza mizelor este un pas esential pentru orice proces de gestionare a riscurilor.

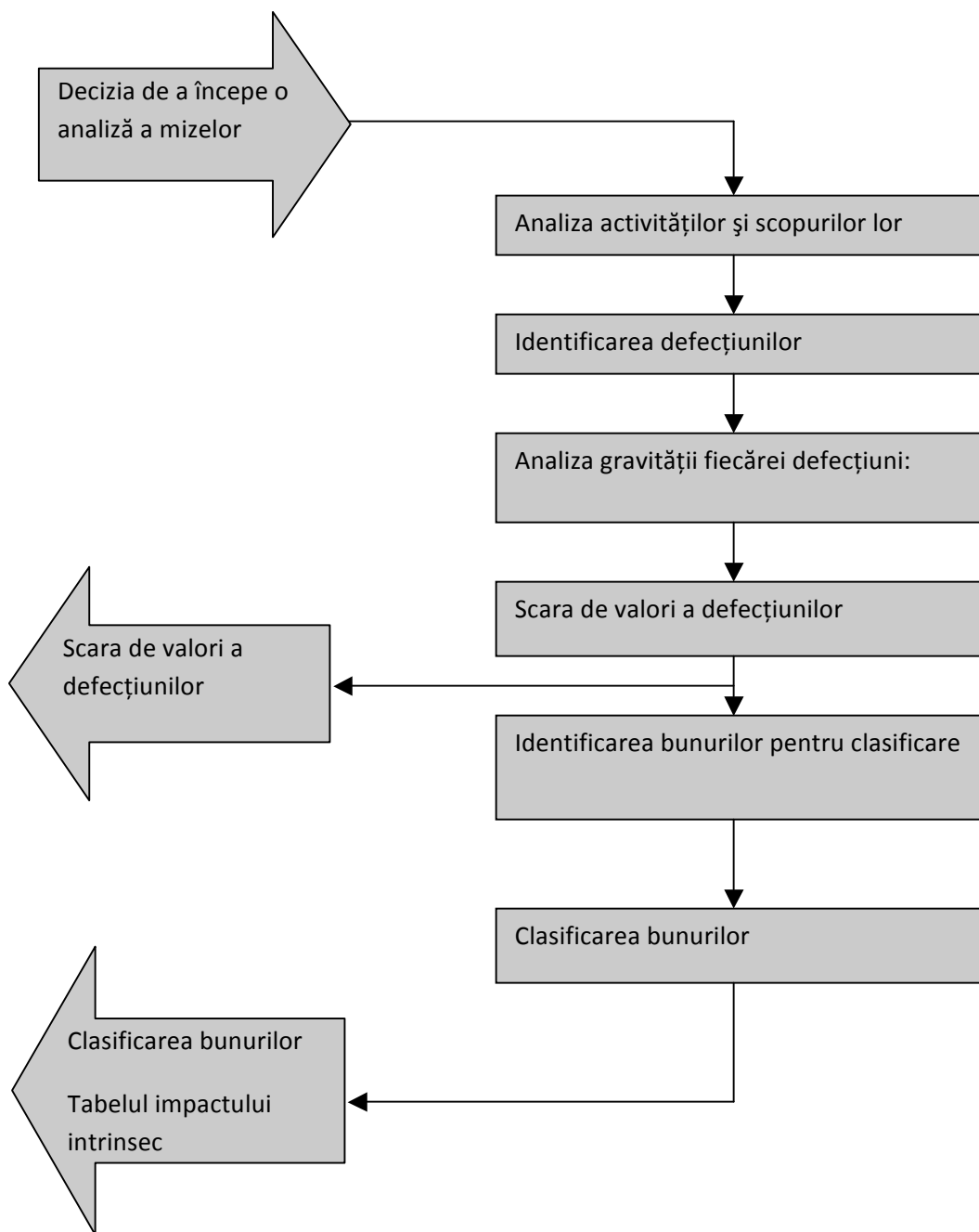
Scopul acestui document este de a completa “ghidul de procesare pentru analiza si gestionare riscurilor” si “ghidul de analiza si gestionare riscurilor”, pentru a oferi asistenta pe durata cursului procesului si pentru a justifica rezultatele. Analiza mizelor trebuie sa ofere 2 seturi principale de rezultate:

- Scara de valori a defectiunilor
- Evaluarea sau clasificarea bunurilor legate de informatie

Din aceste doua seturi de rezultate, este posibila deducerea tabelului impactului intrinsec, folosit pentru evaluarea scenariilor de risc oferite de MEHARI.

Procedura pentru analiza mizelor este descrisa mai jos.

Abordarea MEHARI consta in analizarea activitatilor intreprinderii sau organizatiei, si a proceselor sale de afaceri care au legatura cu informatia, pentru a deduce ce defectiuni ar putea avea loc, si pentru a evalua cat de grave ar putea fi aceste defectiuni. Apoi este posibil sa se evalueze bunurile legate de informatie.



2. Scara de valori a defecțiunilor

Acest proces este conceput pentru a oferi o scara de valori pentru defecțiunile care ar putea afecta semnificativ activitățile unei entități.

Analiza cuprinde 4 etape:

- Analiza activitatilor principale si obiectivele lor

- Identificarea posibilelor defectiuni pentru fiecare activitate, care poate fi realizata la urmatoarele nivele:
 - Tehnic
 - Functional
- O evaluare a nivelului gravitatii defectiunilor, activitate cu activitate
- Determinarea unei scari globale a valorilor pentru entitate.

2.1. Identificarea principalelor activitati si obiectivele lor

Un punct de plecare bun este identificarea activitatilor principale ale domeniului care este analizat, descrierea pe scurt a lor, si identificarea scopurilor sau cel puțin a rezultatelor prevazute.

2.1.1 Rezultatele prevazute

Activitatile vor fi descrise in termeni functionali.

Pe langa o descriere functionala, merita sa se defineasca rezultatele prevazute sau scopurile activitatii. Aceste rezultate dorite ar trebui definite din punctul de vedere al entitatii, si din acela al entitatilor “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 riguroasa si exhaustiva a activitatilor poate fi facuta printr-o analiza a procesului in care actioneaza acestea. Acest lucru presupune identificarea tuturor proceselor din domeniul examinat, chiar sub-divizandu-le in atatea sub-procese cat este nevoie pentru a scoate la suprafata variatele dependinte si rezultate intermediare.

Experienta arata ca o abordare globala si mai intuitiva, daca are un nivel destul de inalt desponsorizare a managementului, poate identifica rapid principalele functii si scopurile lor. Acest lucru este destul de suficient pentru nevoile aceste abordari.

Abordarea este astfel bazata pe interviuri individuale (intre 60 si 90 de minute) cu manageri responsabili pentru activitati diferite in intreprindere sau organizatie.

2.2. Identificarea potentialelor defectiuni

Odata ce activitatile sunt identificate, defectiunile potentiale sau suspectate asociate cu ele ar trebui scoase la lumina.

2.2.1. Rezultatele prevazute

Descrierea defectiunilor ar trebui sa fie de asa natura incat gravitatea sa poata fi evaluata. Totusi, ar trebui mentionat ca o defectiune poate fi descrisa in mai multe moduri:

- La nivelul elementului care deranjeaza sau este deranjat in procesul care este examinat. Acest lucru poate fi, de exemplu, indisponibilitatea sistemului de management al trezoreriei sau baza de date asociata; deci, la un nivel tehnic.
- La nivelul procesului insusi (la nivel functional). De exemplu, incapacitatea de a oferi o privire consolidata asupra necesitatilor trezoreriei.

Aceleasi defectiuni pot fi astfel descrise fie in ceea ce priveste indisponibilitatea a datelor necesare pentru a produce un rezultat specificat, fie in ceea ce priveste incapacitatea de a executa sarcina care ar produce rezultatul. Prima dintre acestea este cunoscuta in MEHARI ca analiza la nivel tehnic a mizelor de securitate, iar cea din urma este cunoscuta ca analiza functionala a mizelor de securitate.

2.2.1.1. Potentiale defectiuni identificate la nivel functional

La nivelul functional, scopul este de a identifica potentialele defectiuni care au un impact significant in activitatile intreprinderii. Acestea vor fi de obicei defectiuni ale proceselor. Urmatoarele criterii generice de profil ale defectiunii procesului vor fi valabile de obicei:

- **Sincronizare incorecta:** sarcinile sau activitatile care sunt planificate nu sunt terminate la timp;
- **Lipsa concordantei:** sarcinile sau activitatile care sunt planuite nu sunt terminate in conformitate cu specificatiile;
- **Lipsa completitudinii:** sarcinile sau activitatile care sunt planificate sunt doar partial terminate (desi partile terminate sunt conform cu specificatiile);
- **Lipsa corectitudinii:** sunt indeplinite sarcini sau activitati aditionale care erau planificate sau specificate;
- **Lipsa discretiei:** informatia este dezvaluita necorespunzator in timp ce sarcinile sau activitatile sunt indeplinite;
- **Lipsa controlului:** sarcinile sau activitatile sunt indeplinite si terminate dupa cum era planificat dar fara control sau vizibilitate asupra executiei lor.

Este posibil, astfel, descrierea unei defectiuni in ceea ce priveste sarcina sau activitatea implicata de catre tipul de defectiune.

Deasemenea este deseori utile sa se descrie consecintele potentiale, pentru a intelege mai bine gravitatea lor.

Deci, folosind exemplul ipotetic al dezvaluirii necorespunzatoare a salariilor angajatilor, merita sa se identifice consecintele potentiale: actiunea de greva, obligatia de a da numeroase mariri de salariu pentru anumite categorii de personal, de-motivarea personalului, si asa mai departe.

Deasemenea, daca defectiunea inchipuita priveste schimbarile de plata, merita identificarea faptului daca consecintele potentiale implica sau nu fraudarea si pierderea de bani, sau actiunea de

greva din partea personalului (sau de-motivarea acestora), sau nevoia de a face corectii numeroase si complicate.

Fiecare defectiune, la nivel functional, ar trebui descris ca o schimbare a procesului afacerii. Astfel ar trebui descrisa in ceea ce priveste procesul sau activitatea in cauza, precum si tipul de defectiune si tipu de consecinte.

Folosind exemplul managementului de trezorerie, mentionat mai sus:

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

2.2.1.2. Potentiale defectiuni identificate la nivel tehnic

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

Bunurile care sunt asigurate ar putea fi:

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

Defecțiune	Consecințe
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 folosi 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. 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 gravitate 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 parametri 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:

Defecțiune	Nivelul 1	Nivelul 2	Nivelul 3	Nivelul 4 Vital
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 este arătat mai jos, pentru o activitate HR.

Defecțiune	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
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:
 - Modulului 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.

Asa cum este formulat în “MEHARI: Concepte fundamentale și specificații funcționale”, bunurile identificate trebuie să corespundă cu cerințele organizației și să aparțină unor 3 categorii:

- Serviciile (fie generale sau în legătură cu ITC);
- Datele necesare pentru ca serviciile să funcționeze;
- Procesele transversale fie în conformitate cu o reglementare sau pentru managementul securității în sine.

Aceste bunuri sunt denumite “bunuri primare” iar o tipologie este listată mai jos:

Bunuri din categoria Servicii

- Servicii de rețea
- Servicii de aplicații
- Obisnuite/Servicii partajate de birou
- Servicii de sistem obisnuite: emailing, arhivare, printare, editare etc
- Servicii pentru interfața cu utilizatorul siferice (pc, imprimante locale, interfațe specifice etc)
- Servicii de telecomunicații(voce, fax, video-conferințe etc)
- Servicii obisnuite pentru atmosfera de lucru a personalului (birouri, alimentarea cu energie, aer condiționat etc)
- Servicii clasice de mail

Bunuri din categoria Data

- Fișiere de date sau baze de date asociate aplicațiilor
- Schimb de date, ecrane, date individuale sensibile
- Fișiere legate de birou
- Informații scrise sau printate disponibile utilizatorilor și arhive personale
- Mail (clasic sau electronic) și faxuri
- Arhive

Bunuri din categoria procese de management

- Procese legate de legi, regularizări și cerințe contractuale
- Procese pentru managementul securității informațiilor

Bunurile primare corespund cerințelor organizației și la acest nivel va trebui evaluată importanța acestor cerințe, acest nivel va fi folosit pentru evaluarea nivelului de risc. Aceste bunuri trebuie clasificate.

Cunostințe de bază MEHARI 2010 furnizează 3 tabele, numite T1 până la T3, și un exemplu pentru completarea lor este propus mai jos:

Tabel T1		clasificarea datelor																													
Procese de afacere, domenii de activitate sau activitati, Servicii obisnuite	Funcție (descriere)	Date ale aplicatiilor (baze de date)			Date sensibile ale aplicatiilor (mesaje)			Date de birou partajate			Date de birou personale			Documente personale		Documente listate		Posta electronica			Fax			Documente arhivate		Arhive digitale			Date online (intern sau extern)		
		A	I	C	A	I	C	A	I	C	A	I	C	A	C	C	A	I	C	A	I	C	A	C	A	I	C	A	I	C	
		D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D04	D04	D05	D07	D07	D07	D08	D08	D08	D09	D09	D10	D10	D10	D11	D11	D11	
Procese de business																															
Domain 1 : Resurse Umane		2	3	2	2	3	2	1	1	3	1	1	3	2	1	2	1	1	2	1	1	2	2	1	1	1	3	1	1	2	
Domain 2 : Managementul Vanzarilor		2	2	4	2	2	4	1	3	3	1	3	3	1	3			3	2	4	3	2	4	1	3	1	3	3	2	4	
Domain 3 : Planificare Strategica							2	2	3	2	2	3	1	3	3	2	3	3	2	3	3	1	3	2	2	3	2	3	3	3	
Domain 4 : Finante & Contabilitate		2	2	3	2	2	3				2	2	3	3		2										3					
Domain 5		2	3	1	2	3	1	2	3	1	2	3	1	2	3	1									2	3	1				
Domain 6 : Proiecte asistate de calculator		3	3	3	3	3	3	3	3	3	3	3	3	3																	
Domain 7 : Site web pentru ecommerce		3	3	1	3	3	1	1	1	1	1	1	1	1																	
.../...																															
Domain N																															
Procese transversale																															
Politici & management general																															
Clasificare		3	3	4	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	4	2	3	3	3	3	4	

Tabel 1 Clasificarea valorilor tip data

Tabel T2		clasificarea serviciilor																	
Procese de afacere, domenii de activitate sau activitati, Servicii obisnuite	Funcție (descriere)	Servicii de retea extinse		Servicii LAN		Servicii ale aplicatiilor			Servicii de birou partajate		Echipament la dispozitia utilizatorilor	Servicii IT		Servicii de editare web		Servicii comune, mediul de lucru		Servicii telecom	
		A	I	A	I	A	I	C	A	I	A	A	I	A	I	A	A	I	
		R01	R01	R02	R02	S01	S01	S01	S02	S02	S03	S04	S04	S05	S05	G01	G02	G02	
Procese de business																			
Domain 1 : Resurse Umane		1	1	2	3	2	3	1	1	1	1	1	1	1	1	1	1	1	1
Domain 2 : Managementul Vanzarilor		2	2	2	2	2	2	4	1	3	1	3	2	3	2	3	3	2	
Domain 3 : Planificare Strategica				2	2			2	2	2									
Domain 4 : Finante & Contabilitate		2	2	2	2	2	2	3											
Domain 5		2	3	2	3	2	3	1	2	3	2								
Domain 6 : Proiecte asistate de calculator		3	3	3	3	3	3	3	3	3	3								
Domain 7 : Site web pentru ecommerce		3	3	3	3	3	3	1	1	1	1								
.../...																			
Domain N																			
Procese transversale																			
Politici & management general																			
Clasificare		3	3	3	3	3	3	4	3	3	3	3	2	3	2	3	3	2	

Tabel 2 Clasificarea valorilor tip servicii

Tabel T3		Clasificarea conformitatii cu legile si alte norme , in legatura cu:						
Procese de afacere, domenii de activitate sau activitati, Servicii obisnuite	Funcție (descriere)	Protectia informatiilor personale		Comunicarile financiare	Controlulu contabilitatii digitale	Proprietatea intelectuala	Protectia sistemelor informationale	Siguranta persoanelor si a mediului de lucru
		E	E	E	E	E	E	
		C01	C02	C03	C04	C05	C06	
Procese de business								
Domain 1 : Resurse Umane		3		1	2	3	2	2
Domain 2 : Managementul Vanzarilor		2		2	2	2	3	
Domain 3 : Planificare Strategica		2			2	2	3	
Domain 4 : Finante & Contabilitate		2		2	3		3	2
Domain 5		2			2		2	
Domain 6 : Proiecte asistate de calculator						3	3	3
Domain 7 : Site web pentru ecommerce		3		3	3	2	3	2
.../...								
Domain N								
Procese transversale								
Politici & management general								
Clasificare		3		3	3	3	3	3

Tabel 3 Clasificarea proceselor de management

3.1.2. Identificarea elementelor legate de politica de securitate a companiei

Este posibil întotdeauna ca anumite servicii obișnuite să nu fie identificate ca și elemente critice în timpul analizei proceselor afacerilor. Totuși, ar putea fi critice (într-o măsură mai mică sau mai mare) pentru întreprindere sau organizație ca un tot.

Acesta ar fi cazul în care, de exemplu, ele ar putea influența planificarea sau dezvoltarea strategiei IT, sau când ele ar putea avea impact asupra imaginii profesionale a organizației sau suportului ei de servicii, fie intern, fie extern.

Aceste servicii comune ar trebui identificate și clasificate, doar pentru procesele afacerii menționate mai sus, permițând o privire corporativă asupra cerințelor de securitate.

3.2 Criteriile de clasificare

Pierderea disponibilității, integrității, sau a confidențialității unui bun poate avea Consec

vențe 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.

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

Pentru servicii, principală preocupare o reprezintă pierderea disponibilității sau a integrității. Totuși, confidențialitatea poate reprezenta și ea o preocupare pentru anumite aplicații care oferă avantaj competitiv pentru entitate.

Pentru respectarea legilor, reglementări sau cerințe contractuale, criteriul de clasificare E (“eficientă”) se aplică, așa cum este exemplificat în tabelul T3.

3.3. Procesul de clasificare

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 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 bunurilor la nivel corporativ

Deasemenea, pentru o viziune a corporatiei, este necesara asumarea consecintelor unei degradari a bunurilor independent de fiecare domeniu de afaceri individual.

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.

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.

Procesul pentru completarea automată a tabelului impactului intrinsec beneficiază de tabelele clasificării bunurilor (T1 până la T3) care au fost definite și descrise în secțiunea precedentă.

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

Defecțiuni	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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.	Indisponibilitate a pe termen lung a sistemului de memento.		

2. Strategie – Indicații generale – Management și urmărire

Defecțiuni	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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		

Coruperea datelor de raportare și a rapoartelor lunare	Coruperea datelor elementare sau informații mărite pe baza unor date elementare.		
--	--	--	--

3. Dezvoltarea afacerii – managementul clientului

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

4. Cercetare și dezvoltare

Defecțiune	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
Dezvăluirea informațiilor tehnice	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.	
Încălcarea acordurilor de confidențialitate		Încălcarea acordurilor de confidențialitate cu partenerii	Încălcarea acordurilor de confidențialitate cu furnizorii cheie de tehnologie	

<i>Pierdere expertizei</i>			Pierdere arhivelor a memorandumurilor și a buletinelor tehnice privind dezvoltarea tehnică.	
----------------------------	--	--	---	--

5. Managementul procesului industrial – Proiecte pentru evoluție - Întreținere

Defecțiune	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<i>Pierdere arhivelor de documente a proiectului de evoluție Pierdere documentației tehnice pentru echipamentul existent</i>	Pierdere arhivelor proiectului pe durata de viață a proiectului. Pierdere copiilor în original a planurilor echipamentului care au fost aprobate de către autoritățile competente.	Pierdere totală a arhivelor pe termen lung privind echipamentul și modificările făcute la acesta.		
<i>Defecțiune 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 proiect 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

Defecțiune	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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	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>Uneltele 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)

Defecțiune	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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	Pierdere 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	

8. Managementul reclamațiilor – aspecte legale și penale

Defecțiune	Nivelul 1 Nesemnificati	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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

Defecțiune	Nivelul 1 Nesemnificati	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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 (calculare 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

Defecțiune	Nivelul 1 Nesemnificativ	Nivelul 2 Grav	Nivelul 3 Foarte grav	Nivelul 4 Vital
<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
Date și informații				
D01	Fișiere de date sau baze de date accesate de aplicații			
D02	Fișierele și datele office comune			
D03	Fișiere office personale (pe PC, echipamente 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, date individuale sensibile			
D07	Poșta electronică			
D08	Scrisori și mesaje fax (postal)			
D09	Documente sau arhive patrimoniale folosite ca dovezi			
D10	Arhive IT			
D11	Date și informații publicate pe site-uri publice sau interne			
Valori servicii		A	I	C
Servicii Generale				
G01	Spatiul de lucru al utilizatorului și mediul de lucru	3		
G02	Servicii de telecomunicații (voce, fax, audio & videoconferință etc.)	3	2	
Servicii IT și de rețea				
R01	Servicii de rețea extinse	3	3	
R02	Servicii LAN	3	3	
S01	Servicii furnizate de aplicații	3	3	4
S02	Servicii comune de birou (servere, management documente, imprimante comune etc.)	3	3	

S03	Echipeamente la dispozitia utilizatorilor (statii de lucru, imprimare locale, periferice, interfete specifice etc.) NOTA: se aplica in cazul pierderilor masive, nu doar la cativa utilizatori	3		
S04	Servicii comune, mediul de lucru: mesagerie, imprimare, arhivare, editare etc.	3	2	
S05	Servicii de editare web (interne sau publice)	3	2	
Valori de tip procese de management		E		
Procese de management pentru conformarea legală și reglementară				
C01	Conformarea la legi și reglementări privind protecția vieții private			
C02	Conformarea la legi și reglementări privind comunicarea financiară			
C03	Conformarea la legi și reglementări privind controlul financiar digital			
C04	Conformarea la legi și reglementări privind drepturile de proprietate intelectuală			
C05	Conformarea la legi și reglementări privind protecția sistemului informațional			
C06	Conformarea la legi și reglementări privind punerea în pericol a personalului și a siguranței publice și a mediului			

In spiritul diseminarii



CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris France
☎ 01 53 25 08 80
clusif@clusif.asso.fr

www.clusif.asso.fr