METODE

MEHARI 2010

Ghid de prelucrare pentru analiza si managementul riscului

August 2010

CLUSIF

Comisia Metodelor

Va rugam sa postati intrebarile si comentariile Dvs. pe forumul: http://mehari.info/

Clubul Francez al Securitatii Informatiei

MULȚUMIRI

Traducerea în limba română a fost realizată de **Pricop Vlad Florian**, student al 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

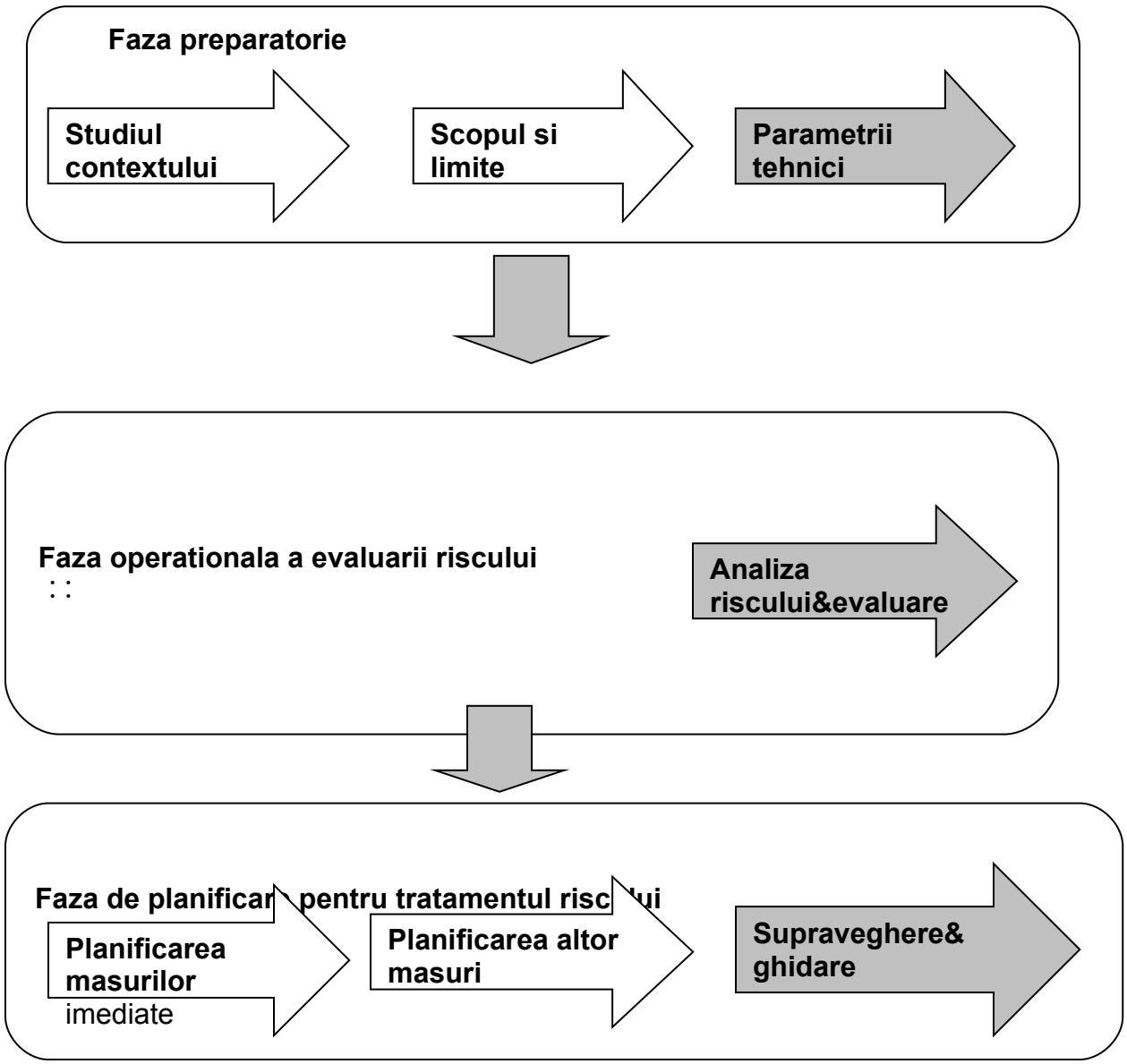
Introducere

Acest ghid prezinta procesarea completa pentru analiza riscului si tratament si descrie diferitii pasi pe care ii implica.

Se bazeaza pe folosirea bazei de cunostinte Mehari 2010.

Prezentarea generala a procesului complet

Abordarea MEHARI implica trei faze, asa cum se ilustreaza in diagrama de mai jos:



1. Faza de pregatire

Faza de pregatire este subdivizata in trei pasi principali. In mod ideal, acestia ar trebui sa fie efectuati unul dupa altul, dar acest lucru nu este absolut necesar.

Pasii sunt:

1.1. Evaluarea contextului

1.1.1. Contextul strategic

1.1.2. ccntextul tehnic

1.1.3. Contextul structural

1.2. Determinarea scopului si a limitelor pentru analiza riscului si tratamentul operational

1.2.1. Perimetrul tehnic

1.2.2. Perimetrul organizational

1.2.3. Structura de ghidaj

1.3. Stabilirea parametrilor principali ai analizei riscului

1.3.1. Tabelul acceptarii riscului

1.3.2. Tabelul expunerii naturale

1.3.3. Tabelul evaluarii riscului

1.1 Evaluarea contextului

1.1.1 Evaluarea contextului strategic

Obiective

Stabilirea unui numar de puncte care trebuie clarificate si de care trebuie sa se tina cont pentru analizarea riscului si pentru tratament.

Trebuie luate in considerare urmatoarele elemente:

- Pozitionarea strategica a entitatii pe piata proprie (pentru entitatile comerciale) sau structura sa intr-un context politic (pentru organizatii si servicii publice):
    - Pozitia pe piata (dominanta sau nu)
    - Natura competitivaa activitatii
    - Praguri critice ale serviciilor furnizate
    - Focusarea media asupra incidentelor sau defectiunilor
    - Etc.

- Constrangeri care cantaresc in operarea si structura entitatii
    - Constrangeri legale
    - Constrangeri de reglementare
    - Reguli de urmat

- Politica de securitate a informatiei

    - Scopurile securitatii (daca acestea exista)
    - Rolul analizarii riscului si a tratamentului in politica securitatii
    - Entitatii care solicita analiza si tratamentul riscului
    - Suport de management

Premise

Pentru inceperea acestei sarcini, este important ca misiunea analizei riscului si a tratamentul operatiunii sa fie stabilite dinainte.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila cu operatiunea de analiza si tratament a riscului.

Partile interesate sunt:

- Manageri de business
- Management general
- Departamentul legal (constrangeri legale)
- CISO

Livrabil

Livrabil: este un document care sintetizeaza variatele obiective declarate.

Procesul – ghid de implementare

Procesul implica urmatoarele:

- O colectie de elemente valabile la obiectivele declarate
- Crearea unui rezumat
- Aprobare din partea Comitetului de Management sau direct de la Managementul General.

1.1.2 Evaluarea contextului tehnic

Obiective

Colectarea si stabiliarea datelor si a informatiilor tehnice care vor fi necesare pentru analiza riscului si pentru tratament.

Trebuie luate in considerare urmatoarele elemente:

- Arhitectura sistemului informational
    - Arhitectura retelei
    - Arhitectura sistemelor

    - Arhitectura aplicatiei
    - Cartografiere globala

- Planuri pentru evolutia tehnica pe termen scurt, mediu si lung
    - Planuri de dezvoltare
    - Solutii pentru durabilitatea operatiunilor
- Furnizori externi cruciali
    - Furnizori de servicii structurale (acces la retea si servicii, management al facilitatilor etc.)
    - Furnizori de software
    - Furnizori ocazionali de servicii (mentenanta, asistenta etc.)

Premise

Cartografierea pre-existenta sau, cel putin, un inventar actualizat al echipamentelor IT, sistemelor si aplicatiilor.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila cu analiza riscului si cu operatiunile de tratament, posibil cu delegare pentru un membru al echipei lui/ei.

Partile implicate sunt:

- CIO (Chief Operation Officer)
- Directorul retelelor/conexiunilor (daca este altul decat CIO)

Livrabil

Livrabil: este cartografia (completa sau rezumata) si o lista (echipamente, aplicatii etc.)

Procesul – ghid de implementare

Procesul implica urmatoarele:

- O colectie cu variatele elemente tehnice disponibile
- Crearea unui rezumat

- Aprobare din partea CIO.

1.1.3 Evaluarea contextului organizational

Obiective

Colectarea si stabilirea datelor si informatiilor despre structura entitatii va fi necesara pentru analiza riscului si pentru tratament.

Urmatoiarele elemente trebuie luate in considerare:

- Tabelul complet al organizatiei
    - Relatii ierarhice
    - Relatii si legaturi functionale.
- Distribuirea responsabilitatilor din ratiuni de securitate
    - Descrirea jobului si asocierea de memo-uri
    - Divizarea responsabilitatii printre manageri de site, managerii de activitate, CIO si CISO.
- Structura de supraveghere
    - Procese existente pentru planuri de actiune propuse sau aprobate
    - Stabilirea modurilor de operare ale structurii de supraveghere.

Premise

Existenta unui tabel complet al organizatiei si note referitoare la functii.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si de operatiunile de tratament, posibila delegare catre o persoana din echipa lui/ei.

Partile interesate sunt:

- Managerul de Resurse Umane sau managementul organizatiei
- Managerul financiar sau ofiterul administrativ
- CISO.

Livrabil

Livrabil: este un rezumat cu structura entitatii si distributia responsabilitatii in termeni de securitate a informatiei si implementare a planurilor de actiune corectoare.

Procesul – ghid de implementare

Procesul implica urmatoarele:

- Colectarea variatelor elemente tehnice disponibile
- Crearea unui rezumat
- Aprobarea din partea managementului general.

1.2 Stabilirea scopului si a granitelor pentru analiaza riscului si operatiunea de tratament

1.2.1 Perimetrii tehnici ai analizei riscului si tratamentului

Obiective

Stabilirea formala a scopului tehnic pentru initierea operatiunii de analiza a riscului si pentru tratament.

Trebuie luate in considerare urmatoarele elemente:

- Perimetrul geografic
    - Situri/locatii
    - Tari, daca este nevoie
- Sisteme de informatii implicate
    - Sisteme de informatii generale
    - Excluderea (sau nu) a sistemelor de managemetn al proceselor industriale
    - Excluderea (sau nu) a sistemelor asistate de computer
    - Etc.
- Tipul informatiilor media implicate
    - Media digitale
    - Media scrisa sau vorbita
    - Media audio

Premise

Existenta unui rezumat al cartografiei sistemului informational.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila cu analiza riscului si operatiunile de tratament.

Partile interesate sunt:

- Managementul general sau clientul care a comandat misiunea
- CISO.

Livrabil

Livrabil: este un rezumat al scopului tehnic al analizei riscului si operatiunilor de tratament.

Procesul – ghid de implementare

Procesul implica urmatoarele:

- O colectie a variatelor optiuni si alegeri ale clientului
- Crearea unui rezumat
- Aprobare din partea managmentului general

1.2.2. Perimetrul organizational al analizei riscului si tratamentului

Obiective

Stabilirea formala a scopului analizei riscului si tratamentului pentru operatiunea planificata.

Urmatoarele elemente trebuie luate in considerare:

- Petrimetrul activitatii
    - Activitatile implicate
    - Filiale, unitati sau servicii (acolo unde sunt necesare)
    - Limitarea la unul sau mai multe tipuri de risc (frauda sau divulgare, de exemplu).

Premise

Existenta unui sumar al structurii entitatii.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si opreratiunea de tratament.

Partile interesate:

- Managementul general sau clientul
- CISO.

Livrabil

Livrabil: este sumarul scopului structural al analizei riscului si operatiunii de tratament.

Procesul – ghid de implementare

Procesul va implica urmatoarele:

- Un studiu al variatelor optiuni si alegeri ale clientului
- Crearea unui rezumat
- Aprobarea din partea managementului.

1.2.3 Structura de supraveghere a operatiunii

Obiective

Stabilirea formala a structurii de supraveghere a operatiunii si a relatiei dintre analiza riscului si echipa de tratament si client sau managementul general.

Trebuie luate in considerare urmatoarele elemente:

- Moduri de structurare si operare a Comitetului de Supraveghere pentru operatiune
    - Participanti
    - Program de intalniri
- Tipuri de metode de aprobare si livrare

Premise

Existenta unui sumar al structurii entitatii.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si de operatiunea de tratament.

Partile interesate sunt:

- Managementul general sau clientul
- CISO

Livrabil

Livrabil: este un rezumat al structurii de supraveghere a analizei riscului si operatiunii de tratament. Ar trebui organizata o intalnire initiala cu Comitetul de Supraveghere.

Procesul – ghid de implementare

- Procesul impu despre variatele optiuni si alegeri ale clientului
- Crearea unui rezumat
- Aprobarea din partea managementului general.

1.3 Stabilirea parametrilor tehnici ai analizei riscului

Inainte de analizarea propriu-zisa a riscului, urmatorii parametrii trebuie stabiliti:

- Tabelul de acceptabilitate a riscului
- Expunerea naturala
- Un tabel cu evaluarea riscului.

1.3.1 Tabelul stabilirii acceptabilitatii riscului

Obiective

Stabilirea formala a tabelului acceptabilitatii riscului, folosit dupa aceea pentru a stabili daca scenariul riscului este tolerabil sau nu.
Tabelul este prezentat in "Mehari 2010: ghid de analiza a riscului si tratament".

Premise

Existenta unui rezumat despre structura de supraveghere pentru analiza riscului si tratament.
Aditional, Comitetul de Supraveghere, care este o parte interesata cheie in sarcina, trebuie sa aiba o intelegere initiala a modelul de risc Mehari.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si tratament.
Partile interesate sunt:

- Managemntul general sau clientul
- Comitetul de Supraveghere a operatiunii
- CISO

Livrabil

Livrabil: reprezinta tabelul de acceptabilitate a riscului si orice alta terminologie asociata cu fiecare categorie de risc.

Procesul – ghid de implementare

Procesele implicate sunt:

- Elaborarea unui tabel de acceptabilitate a riscului
- Aprobarea din partea managementului general.

Nota: acest draft poate fi elaborat dupa tabelul prezentat in baza Mehari si oferit ca model in "Mehari 2010: ghid de analiza si tratament al riscului". O aprobare din partea managementului general este necesara.

1.3.2 Tabel in care se stabileste expunerea naturala

Obiective

Stabilirea formala a unui tabel cu expunerea naturala sau un tabel cu probabilitatile intrisece folosite apoi pentru stabilirea potentialului intrisec al scenariului de risc in baza de cunostinte.

Acest tabel este prezentat in "Mehari 2010: ghid de analiza a riscului si tratament" si in "Mehari 2010 Conceptii fundamentale si specificatii functionale".

Premise

Comitetul de Supraveghere, care reprezinta o parte interesata cheie in aceasta sarcina, trebuie sa aiba o intelegere initiala a modelului de risc Mehari.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si operatiunea de tratament.

Partile interesate sunt:

- Comitetul de Supraveghere a operatiunii
- CISO

Livrabil

Livrabillitatea este tabelul de acceptabilitate a riscului si orice alta terminologie asociata cu fiecare categorie de risc.

Procesul – ghid de implmentare

Procesul implica urmatoarele:

- Elaborarea unui tabel al expunerii naturale
- Aprobare din partea Comitetului de Supraveghere.

Nota: acest draft poate reprezenta baza tabelului expunerii naturale prezentat in baza de cunostinte Mehari si oferit ca exemplu in "Mehari 2010: ghid de analiza a riscului si tratament". Aprobarea din partea Comitetului de Supraveghere este necesara.

1.3.3 Stabilirea unor tabele de evaluare pentru potentialitate reziduala si impact

Obiective

Stabilirea formala a unor tabele care sa permita evaluarea potentialitatii reziduale si a impactului, bazata atat pe potentialul intrisec/impact, cat si pe reducerea factorilor de risc in fiecare din scenariile din baza de cunostinte.

Aceste tabele sunt prezentate in "Mehari 2010: ghid de analiza a riscului si tratament" si in "Mehari 2010 – Concepte fundamentale si specificarii functionale".

Premise

Aditional, Comitetul de Supraveghere, care reprezinta partea interesata cheie in aceasta sarcina, trebuie sa aiba a priori o intelegere a modelului de risc Mehari.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila cu analiza riscului si operatiunea de tratament.

Partile interesate sunt:

- Comitetul de Supraveghere a operatiunii

- CISO

Livrabil

Livrabil: reprezinta o serie de tabele de evaluare a riscului.

Procesul – ghid de implementare

Procesul implica urmatoarele:

- Elaborarea unor tabele (3 pentru evaluarea potentialitatii reziduale si 4 pentru evaluarea impactului rezidual).
- Aprobare din partea Comitetului de Supraveghere.

Nota: aceste drafturi pot folosi tabelele de baza prezentate in baza de cunostinte Mehari si oferite ca exemplu in "Mehari 2010: ghid de analiza a riscului si tratament".
Este recomandata aprobarea din partea Comitetului de Supraveghere.

2. Analiza riscului-faza operationala

Operatiunea analizei riscului include trei mari pasi.

Acestia sunt:

2.1 Analiza intereselor si clasificarea activelor

2.1.1 Scala valorii de defectiune

Obiective

A stabili oficial interesele de securitate pentru fiecare activitate a unei entitati, pentru a fi utilizate mai apoi pentru clasificarea calitatilor.

Scopul si obiectivele scalei de valori ale defectiunii sunt descrise in "Mehari 2010 – *Stakes Analysis and Classification guide*".

Pentru fiecare activitate, scala valorii de defectiune este utilizata pentru a evidentia :

- Defectiuni periculoase
- Criterii calitative sau cantitative pentru evaluarea gravitatii acestor defectiuni pe o scala de la unu la patru.

Premise

Pentru a initia aceasta sarcina, este important sa fie stabilita o ordine de lucru pentru operatiunea de analiza a intereselor.

Este recomandat ca aceasta sarcina sa fie precedata de o intalnire pentru a se identifica procedura si perspectivele de gestionare/administrare.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de operatiunea de analiza a riscului si tratament.

Partile interesate sunt:

- Managerii de activitate
- Managementul general
- Ofiterul Sef de Securitate a Informatiilor.

Livrabil

Livrabil: este scala valorii de defectiune pentru o entitate.

Procesul- Ghid de implementare

Descris in intregime in "Security Stakes Analysis and Classification guide", procesul implica urmatoarele:

- O intalnire de inceput
- Intalniri cu managerii de activitate pentru evidentierea potentialelor defectiuni si criteriul pentru a evalua cat de serioase sunt acestea
- Rezumatul fiecarei actiuni
- Un sumar global pentru entitate
- Aprobarea de catre Comitetul de Gestionare sau direct de catre General Management.

2.1.2 Clasificarea activelor

Obiective

Clasificarea fiecarui set de active in functie de cat de sensitive sunt acestea.
Seturile de active folosite in baza de cunostinte MEHARI 2010 sunt categorii de activitati ce tin de activele elementare, conform definitiei din "Mehari 2010 – Concepte fundamentale si specificatii functionale ".

Activele ar trebui clasificate in functie de Disponibilitate, Integritate si Confidentialite.

Clasificarea este utilizata pentru a intregi tabelurile de clasificare – T1, T2 si T3 – infatisate in "Mehari 2010 – Security Stakes Analysis and Classification". Fiecare celula din tabelurile T1 si T2 ar trebui sa indice cel mai inalt nivel de gravitate inerent intr-un anume tip de deteriorare (indisponibilitate, pierderea de integritate sau confidentialitate) pentru fiecare tip de activ si actiune implicata (specificata in fiecare linie a tabelului). Celulele din tabelul T3 indica nivelul de eficacitate necesar proceselor de gestionare in conformitate cu legile si regulamentele.

Premise

Este puternic recomandabil, chiar esential, ca scala valorilor de defectiune sa fie stabilita anticipat. Activele clasificate imediat pot afecta procesul de analiza a riscului.

Participanti si partile interesate

Organizatorul acestei sarcini este persoana responsabila de operatiunea de analiza a riscului si de tratament.

Partile interesate sunt:

- Managerii de activitati
- Ofiterul sef de informatii
- Ofiterul Sef de Securitate a Informatiilor.

Livrabil

- Livrabilele sunt de la T1 la T3 tabelele de clasificare.

Procesul-Ghid de implementare

Procesul ,descris in "stakes and classification guide" include urmatoarele:

- Finalizarea tabelelor T1 pana la T3 prin indicarea liniilor corespunzatoare diferitelor domenii de activitate incluse pe scala de valori ale defectiunii:

- Fiecare celula din tabel indica un tip de deteriorare (indisponibilitate, pierderea integritatii, a confidentialitatii) dupa tipul de active (titlul coloanei) si dupa activitate (enumerata in fiecare liniei a tabelului).

Este necesar sa se determine:

- Daca aceasta deteriorare poate duce la una sau mai multe defectiuni enumerate pe scala de valori ale defectiunii.
- Daca poate duce la una sau mai multe defectiuni, atunci care este cel mai inalt nivel posibil gravitate ingrijoratoare ? Cel mai inalt nivel va fi clasificat/introdus in celula tabelului.
- Daca nu, un "1" (reprezentand nivelul minim de gravitate) poate fi introdus in celula tabelului.
- Introducerea, utilizand aceeasi metoda, a liniei ce indica gestionarea sau vederea de ansamblu a Ofiterului Sef de Informatii (aceasta poate indica un nivel mai inalt al nevoii generale decat ansamblul nevoilor pentru fiecare activitate).
- Aprobarea de catre Comitetul de Gestiune.

2.1.3 Tabelul de impact intrinsec

Completarea tabelului de impact intrinsec, folosit pentru a evalua situatiile de risc ale bazei de cunostinte.
Baza de cunostinte MEHARI (a se vedea "MEHARI Risk analysis and treatment guide") contine scenarii (peste 800 in editia din 2010) care se refera specific la tipul de active si impactul lor intrinsec.
Valorile impactului intrinsec din scenariul de risc al bazei de date sunt incluse in tabelul de impact intrinsec.

Premise
Tabele de clasificare T1 si T3 trebuie completate anticipat (a se vedea paragraful precedent).

Participanti si partile interesate
Organizatorul aceste sarcini este persoana responsabila de operatiunea de analiza si tratare a riscului, eventual delegate unui mebru al echipei lui/ei.
Partile interesate sunt :

- Managerii de activitate
- Departamenul legal
- Departamentul de comunicatii
- Ofiterul Sef de Securitate a Informatiilor

Livrabil

Livrabil: este tabelul de impact intrinsec (a se vedea fila "Classif" din baza de cunostinte).

Procesul - Ghid de implementare

Optiunea de baza, descrisa mai jos,implica completarea tabelului standard de impact intrinsec. Procesul implica urmatoarele:

- Liniile din primele doua sectiuni ale tabelului de impact intrinsec (service-/data related assets) corespund unui tip de activ, si asupra acestui punct sunt trei valori ale impactului (A,I si C) de introdus.Fiecare valoare este cea mai inalta posibil pentru fiecare din coloanele fie ale tabelului T1 sau T2 (fiecare coloana contine un tip de defectiune dat, pentru un tip de activ dat). Proprietatea calcului automat continuta de Mehari 2010 poate fi folosita pentru a completa automat tabelul pe baza lui T1 si T2.

- Pentru ultima sectiune, ce contine numai o coloana, evalueaza impactul de non-conformitate, implicand fiecare din procesele de gestiune enumerate. Aceasta ar trebuie realizata cu managerii de activitate si cu asistenta departamentelor (legal si de comunicatii).

- Aprobarea de catre Comitetul de Gestiune.

2.2 Evaluare calitatii serviciilor de securitate

Obiective

Serviciile de securitate sunt caracteristici ce pot implica tipuri diferite de echipament si punerea in aplicare de strategii in cadrul aceleasi companii. Aceste diferente trebuie prin urmare, sa fie considerate parti ale aceluiasi serviciu, necesitand evaluari diferentiate. Scopul acestui demers este de a indentifica diferitele variante ce necesita evaluari separate.

Premise

O imagine generala dinainte, a contextului tehnic si organizational (pasii 1.1.2 si 1.1.3) este necesara.

Participanti si partile interesate

Organizatorul aceste sarcini este persoana responsabila de operatiunea de analiza si tratare a riscului, eventual delegate unui mebru al echipei lui/ei.

Partile interesate sunt :

- Clientul
- Managerul de servicii generale,
- Ofiterul sef de informatii,
- Ofiterul Sef de Securitate a Informatiilor.

Livrabil

Livrabil: reprezinta o schema de verificare care enumera diferitele variante pe domeniu de securitate.

Procesul-Ghid de implementare

Detalii de luat in considerare si sfaturi despre conceperea schemei de verificare sunt descrise in “Mehari 2010 – Evaluation Guide for Security Services “ .

Procesul implica urmatoarele :

- Pentru fiecare domeniu de securitate, o analiza asupra numarului de variante este necesara.

- Aprobarea intregii scheme de verificare de catre persoana responsabila de operatiunea de analiza a riscului.

2.2.2 Evaluarea calitatii serviciilor de securitate

Obiective

Realizarea unei revizuiri a nivelului calitatii fiecarei variante a serviciilor de securitate. Aceasta apreciere globala este utilizata pentru a evalua factorii de minimalizare a riscului in timpul proceselor de analiza si evaluare.

Premise

O imagine generala dinainte, a contextului tehnic si organizational (pasii 1.1.2 si 1.1.3) este necesara.Schema de verificare trebuie sa fie deja completata.

Participanti si partile interesate

Organizatorul aceste sarcini este persoana responsabila de operatiunea de analiza si tratare a riscului.

Partile interesate sunt :

- Managerii din departamentele tehnice (servicii generale, IS, retele, telecomunicatii, *user equipment pools*, securitatea aplicatiilor, dezvoltarea aplicatiilor, etc.) sau manageri din departamente administrative (legal, organizational, etc.)
- Ofiterul sef de informatii,
- Ofiterul Sef de Securitate a Informatiilor.

Livrabil

Livrabil: reprezinta un set de fisere de diagnoza (una pe domeniu de securitate si pe varianta de categorie) sustinuta in baza de date Mehari (editia din 2010 contine 14 categorii de evaluari).

Aceste fisiere pot fi insotite de rezumate ca mijloc de comunicatie (vizualizari radar,de exemplu).

Procesul-Ghid de implementare

Detalii de luat in considerare in timpul procesului de evaluare se regasesc in "Mehari 2010 – Evaluation Guide for Security Services" .

Procesul implica urmatoarele:

- O evaluare a fiecarei variante a fiecarui domeniu de securitate de catre managerii responsabili.
- Orice corectura necesara sau ajustare de catre manageri din diferite departamente
- Crearea rezumatelor
- Aprobarea de catre Comitetul de Gestiune.

2.3 Evaluarea riscului

2.3.1 Selectarea scenariilor de risc

Obiective

Selectarea unei serii de scenarii de risc in scopul de a focaliza analiza asupra situatiilor care ar putea fi critice.

Premise

Pasii fazei preparatorii si clasificarea activelor trebuie sa fie dinainte incheiate.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de operatiunea de analiza si tratare a riscului.

Partile interesate sunt :

- Managerii de activitati,
- Ofiterul Sef de Securitate a Informatiilor.

Livrabil

Livrabil: reprezinta un rezumat al optiunilor selectate si o lista a scenariilor ce trebuie analizate in detaliu (in practica, aceasta presupune introducerea in coloana “selectie” a foii de calcul “Scenarii” din baza de cunostinte MEHARI 2010).

Procesul-Ghid de implmentare

Orientarile pentru selectarea scenariilor pot fi gasite in “Mehari 2010 – Analiza de risc si ghid de tratament“.

Procesul implica urmatoarele :

- Determinarea unei strategii de selectare :
    - Scenarii cu un impact intrinsec peste o anumita limita (3,de exemplu)
    - Scenarii cu un nivel de seriozitate intrinseca peste o anumita limita (idem)
    - Scenarii ce afecteaza tipuri specifice de active.
- Aprobarea de catre Comitetul de Gestiune
- Selectia eficienta de scenarii in baza .

2.3.2 Evaluarea riscului

Obiective

O analiza a cat de serioase sunt scenariile de risc selectate , in raport cu starea calitatii

Premise

Toate etapele precedente descrise mai sus trebuie sa fie dinainte incheiate.

Participanti si partile interesate

Organizatorul acestei sarcini este persoana responsabila de operatiunea de analiza si tratare a riscului.

Partile interesate sunt :

- Ofiterul Sef de Securitate a Informatiilor.

Livrabil

Principala livrabila este baza de cunostinte Mehari, care a fost completata si finalizata. Aceasta baza contine rezumate organizate dupa tipul de activ, si tipul de incident. Prezentari aditionale pot fi incluse, cum ar fi cartografierea riscurilor, de exemplu (in ca I, P ca plan) sau orice alt tip de rezumat.

Procesul-Implementarea orientarilor

Orientarile pentru selectarea scenariilor pot fi gasite in "Mehari 2010 – Analiza riscului si ghid de tratament".

Procesul implica urmatoarele :

- Incorporarea rezultatului evaluarii calitatii serviciului de securitate (daca ele nu au fost dinainte introduse corect in baza).

-Analiza scenariilor si , daca este necesar, corectarea factorilor de reducere a riscului daca orice anomalie este detectata.

- Crearea rezumatelor

- Prezentarea catre Comitetul de Gestiune

3. Tratarea riscului si faza planificarii

Faza planficarii si tratarii riscului este compusa din trei mari pasi.

Acestia sunt :

3.1 Planificarea masurilor imediate

3.1.1 Selectarea riscurilor pentru o tratare imediata

3.1.2 Selectarea masurilor pentru o implementare imediata

3.2 Planificarea masurilor specifice contextului

3.2.1 Strategia de prioritate si tratare

3.2.2 Selectarea masurilor si planificarii

3.3 Implementarea supravegherii asupra tratarii riscului

3.3.1 Planificarea supravegherii

3.3.2 Indicatori , dash board si graficul tendintei

3.1 Planificarea masurilor imediate

3.1.1 Selectarea riscurilor pentru tratearea imdediata

Obiective

Selectarea scenariilor de risc cu prioritate ridicata pentru a fi tratate in regim special. Criteriul principal de selectie ar trebui sa fie axat pe cel mai crtitv nivel (nivelul 4), dar alt criteriu poate fi folosit.

Premise

Pasii etapei de analiza a riscului trebuie sa fie dinainte incheiati.

Participanti si persoane interesate

Organizatorul acestei sarcini este persoana responsabila de operatiunea de analiza si tratare a riscului.

Partile interesate sunt :

- Managerii de activitate si cei de afaceri
- Ofiterul Sef de Securitate a Informatiilor

Livrabil

Livrabila reprezinta un rezumat al riscurilor intolerabile necesitand un tratament prioritar.

Procesul-Implementarea orientarilor

Orientarile pentru selectarea scenariilor pot fi gasite in " Mehari 2010 – Risk analysis and treatment guide ".

Procesul implica urmatoarele :

- Determinarea unei strategii de selectare :
  - Scenarii ce prezinta cel mai inalt posibil nivel de risc intrinsec (4)
  - Orice alt criteriu folosit
- Aprobarea de catre managerii de activitate
- Selectia eficienta de scenarii in baza

3.1.2. Selectarea masurilor pentru implementare imediata

Obiective

Oferirea Managementului General a unor solutii imediate pentru reducerea riscurilor considerate intolerabile. Aici, telul nu este neaparat de a face tolerabile riscurile reziduale, dar sa muti riscurile de la nivelul intolerabil (nivel 4) la nivelul inadmisbil (nivel 3). Acestea pot fi reduse mai tarziu la nivelul 1 sau 2.

Premise

Pasii etapei analizarii riscului trebuie terminati dinainte.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si de operatiunea de tratament.

Partile interesate sunt:

- Manageri ai activitatii
- CISO
- Management general

Livrabil

Livrabil: reprezinta o serie de planuri de actiune: unul pentru fiecare risc intolerabil care trebuie redus.

Procesul – ghid de implementare

In cazul riscurilor cu grad mare de intolerabilitate, abilitatea de a rasopunde foarte repede este esentiala.

Procesul implica urmatoarele:

- Determinarea unei actiuni strategice:
    - Evitarea riscului (prin intermediul masurilor strategice)
    - Reducerea riscului (prin intermediul masurilor structurale si tehnice)
- Selectarea unor masuri rapide de implementare
- Planificare si budgetarea costurilor
- Aprobare preliminara din partea managerul de activitate
- Aprobare din partea Comitetului de Management si Managementului General.

3.2. Planificarea masurilor specifice contextului

3.2.1. Tratament strategic si stabilirea prioritatilor

Obiective

Alegerea intre posibilele strategii de tratament si selectarea criteriilor pentru stabilirea prioritatilor, pastrarea in minte ca in general nu este posibil ca toate riscurilor inadmisibile sa fie tratate simultan.

Pe langa o selectie initiala bazata pe seriozitatea riscului (incepand cu nivelul 3 de risc), trebuie luate in considerare urmatoarele:

- Cat de repede pot fi implementate masurile aditionale (care sa produca rezultate rapide si care sa motiveze managerii)
- Eficienta costurilor
- Eficienta timpului
- Resursele umane necesare pentru implementarea planurilor de actiune
- Impactul asupra userilor (pozitiv sau negativ)
- Alegerea unor teme particulare (continuitatea operatiunilor, plan de rezerva, acces controlat etc.)
- Etc.

Premise

Pasii fazei de analiza a riscului trebuie sa fie efectuati dinainte.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza riscului si de operatiunea de tratament.

Partile interesate sunt:

- Managerii de activitate
- CIO
- CISO

Livrabil

Livrabil: reprezinta un rezumat al strategiilor de tratament si al prioritatilor.

Procesul – ghid de implementare

Procesul implica urmatoarele:

- Evaluarea avantajelor si dezavantajelor fiecarei optiuni
- Discutii prelimarii si arbitrarii cu managerii de activitate si cu partile interesate
- Aprobarea din partea Comitetului de Management.

3.2.2 Masuri selective si planificare

Obiective

Ofera planuri de actiune Comitetului de Gestiune (in general pe durata a mai multi ani) pentru a reduce sau a evita riscurile considerate ca inadmisibile (Nivelul 3). Aici, scopul nu este in mod necesar de a trata simultan toate riscurile inadmisibile, dar de a avea un plan global si posibil pe durata a mai multi ani bazat pe stabilirea dinainte a prioritatilor.

Premise

Faza pasilor analizei de risc trebuie sa fie finalizata dinainte.

Participanti si parti interesate

Organizatorul acestei sarcini este persoana responsabila de analiza de risc si operatia legata de tratament.

Partile interesate sunt:

- Managerii de activitate
- CIO
- CISO
- Managementul general;

Livrabil

Livrabil: reprezinta o serie de planuri de actiune, de obicei grupate impreuna in cadrul proiectelor.

Procesul – ghid de implementare

In cazul riscurilor inadmisibile, este esential de a fi capabil de a decide care actiune este necesara din cadrul ciclului uzual decizional.

Procesul implica urmatoarele:

- Selectarea masurilor pentru implementare (cateva strategii sunt posibile de-a lungul acestui proces: de vazut "analiza de risc si ghidul de "tratament");
- Planificarea si costul bugetului;
- Prezentarea obiectivelor in termenii riscului si cum vor evolua de-a lungul timpului;
- Aprobarea preliminara cu activitatea managerilor si CIO-ului;
- Aprobarea Comitetului de Gestiune (bazat pe ciclul arbitrajului uzual).

3.3 Supravegherea implementarii tratamentului riscului

3.3.1 Planificarea supravegherii

Obiective

Pentru a organiza si implementa monitorizarea si supravegherea tratamentului riscului trebuie sa se decida asupra urmatoarelor:

- Supravegherea membrilor Comitetului
- Presedintele
- Programarea unei sedinte
- Sarcinile Comitetului

Premise

Pasii fazei pregatitoare trebuie sa fie realizati dinainte.

Participanti si partile interesate

Organizatorul acestei sarcini este persoana responsabila de analiza de risc si tratamentul operatiei.

Partile interesate sunt:

- Managerii activitatii
- CIO
- CISO

Livrabil

Livrabil: reprezinta un sumar prin care se explica cum este dirijat /controlat managementul riscului / gestiunea riscului.

Procesul – implementarea orientarilor

Procesul implica urmatoarele:

- Organizarea propusa dezvoltata de managerul sarcinilor si CISO
- Selectarea membrilor Comitetului de supraveghere
- Aprobarea de catre Comitetul de Gestiune

3.3.2. Selectarea indicatorilor, tabloul de bord si diagrama tendintelor

Obiective

De a oferi Comitetului de supraveghere o serie de indicatori si o diagrama a tendintelor prin care se pot realiza:

- Verificarea implementarii masurilor decise si evolutia / progresul proiectului;
- Verificarea evolutiei nivelurilor riscului;
- Acordul asupra masurilor corective ce sunt necesare.

Premise

Sarcinile si alcatuirea Comitetului Global trebuie sa fie definit dinainte.

Participanti si partile interesate

Organizatorul acestei sarcini este persoana responsabila analizei de risc si operatiei tratamentului.

Partile interesate sunt:

- Managerii activitatilor
- CIO
- CISO

Livrabil

Livrabil: reprezinta elaborarea unui tabel cu tendinte si o lista de indicatori care vor fi utilizati.

Proces – ghid de implementare

Indicatorii trebuie sa fie selectati pentru a permite o monitorizare pe o perioada scurta de timp (progres, probleme aparute, monitorizarea bugetului, etc.) precum si pentru viziunea completa, pe termen mediu si lung (numarul situatiilor de risc per nivel de risc rezidual, prognoza multi-anuala, etc.).

Procesul implica urmatoarele:

- Selectarea indicatorilor
- Dezvoltarea tablourilor de bord si diagrama tendintelor
- Aprobarea preliminara cu activitatea managerilor si CIO
- Aprobarea Comitetului de Gestiune.

In spiritul diseminarii

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris France
✆ + 33 1 53 25 08 80
clusif@clusif.asso.fr

www.clusif.asso.fr