**Banca MAIB**



|  |  |
| --- | --- |
| Code: |  |
| Version: | 1.1 |
| Date of version: | 23.11.2022 |
| Created by: | Plugaru Victoria, Cucta Maria, Cebotari Dan, Golan Grigore |
| Approved by: | lect. univ. Bulai Rodica |
| Confidentiality level: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 09.11.2022 | 1.0 | Plugaru Victoria, Cucta Maria, Cebotari Dan, Golan Grigore | Schița de bază a documentului |
| 23.11.2022 | 1.1 | Plugaru Victoria, Cucta Maria, Cebotari Dan, Golan Grigore | Formatarea documentului |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[SCOP, OBIECTIVE ȘI UTILIZATORI 3](#_Toc119075053)

[DOCUMENTELE DE REFERINȚĂ 3](#_Toc119075054)

[METODOLOGIA DE EVALUARE A RISCURILOR ȘI DE TRATARE A RISCURILOR 4](#_Toc119075055)

[EVALUARE A RISCURILOR 4](#_Toc119075056)

[PROCESUL 4](#_Toc119075057)

[SCALA DE EVALUARE A RISCURILOR 4](#_Toc119075058)

[ACTIVE, VULNERABILITĂȚI ȘI AMENINȚĂRI 4](#_Toc119075059)

[CONSECINȚE ȘI PROBABILITATEA 5](#_Toc119075060)

[TRATAREA RISCULUI ȘI PLANUL DE TRATARE A RISCULUI 6](#_Toc119075061)

[DECLARAȚIA DE APLICABILITATE 7](#_Toc119075062)

[VALABILITATEA ȘI MANAGEMENTUL DOCUMENTELOR 9](#_Toc119075063)

# SCOP, OBIECTIVE ȘI UTILIZATORI

Scopul acestui document este de a defini metodologia de evaluare și tratare a riscurilor informaționale în banca MAIB și de a defini nivelul acceptabil de risc conform standardului ISO/IEC 27001.

Evaluarea riscurilor și tratarea riscurilor sunt aplicate întregului domeniu de aplicare al Sistemului de management al securității informațiilor (ISMS), adică tuturor activelor care sunt utilizate în cadrul organizației sau care ar putea avea un impact asupra securității informațiilor în cadrul ISMS.

Metodologia de evaluare a riscurilor răspunde următoarelor obiective:

* Formularea unor definiții unice pentru termenii cheie utilizați în evaluarea riscurilor la nivel național;
* Identificarea și descrierea unor scenarii;
* Prioritizarea și selectarea scenariilor care vor fi ulterior incluse în evaluările de risc sectoriale;
* Identificarea și evaluarea principalelor riscuri la nivel național și evaluarea capacităților de intervenție care pot influența derularea/impactul scenariilor.
* Furnizarea unui cadru de analiză pentru autoritățile din domeniu în vederea evaluării de risc pentru hazardurile care le sunt repartizate;
* Crearea unei baze solide pentru ierarhizarea și tratarea riscurilor în vederea abordării nevoilor identificate la nivel național.

Utilizatorii acestui document sunt toți angajații Băncii MAIB care participă la evaluarea riscurilor și la tratarea riscurilor.

# DOCUMENTELE DE REFERINȚĂ

* ISO/IEC 27001 standard;
* ISO/IEC 27005;
* Politica de Securitate a Datelor cu Caracter Personal în cadrul MAIB;
* Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
* Legea nr. 133/2011 privind protecția datelor cu caracter personal;

# METODOLOGIA DE EVALUARE A RISCURILOR ȘI DE TRATARE A RISCURILOR

## EVALUARE A RISCURILOR

### PROCESUL

Evaluarea riscurilor sa realizat urmărind răspunsul la risc într-o ordine de priorităţi şi reprezintă etapa ulterioară identificării riscurilor.

Evaluarea riscurilor constă în:

* Estimarea probabilităţii de materializare a riscurilor;
* Estimarea impactului asupra obiectivelor/activităţilor în cazul materializării riscurilor;
* Evaluarea expunerii la risc - combinaţie între probabilitate şi impact.

Evaluarea riscurilor:

* Sa bazat pe utilizarea unei scale de evaluare;
* A avut în vedere pe toţi cei afectaţi de risc;
* A făcut distincţia între expunerea la risc şi toleranţa la risc.

### SCALA DE EVALUARE A RISCURILOR

Riscurile au fost identificate și analizate în funcţie de nivelul pericolului pe care-l reprezintă pentru compania MAIB. Descrierea riscurilor a fost expusă în matricea probabilităţii şi impactului.

În funcţie de impact, riscul poate fi:

* Înalt;
* Mediu;
* Scăzut.

În funcţie de probabilitate de apariţie riscul poate fi:

* de probabilitate înaltă de apariţie (aproape sigur),
* de probabilitate medie de apariţie (posibil)
* de probabilitate mică de apariţie (rar).

### ACTIVE, VULNERABILITĂȚI ȘI AMENINȚĂRI

Primul pas în evaluarea riscurilor a fost identificarea tuturor activelor din domeniul ISMS – adică a tuturor activelor care au afectat confidențialitatea, integritatea și disponibilitatea informațiilor în organizație. Activele au inclus documente în format hârtie și electronic, aplicații și baze de date, oameni, echipamente IT, infrastructură și servicii externe/procese externalizate. La identificarea bunurilora fost necesar să identificăm proprietarii acestora – persoana sau unitatea organizatorică responsabilă pentru fiecare bun.

Următorul pas a fost identificarea tuturor amenințărilor și vulnerabilităților asociate fiecărui activ. Amenințările și vulnerabilitățile au fost identificate folosind cataloagele incluse în Tabelul de evaluare a riscurilor. Fiecare activ poate fi asociat cu mai multe amenințări și fiecare amenințare poate fi asociată cu mai multe vulnerabilități.

|  |  |  |
| --- | --- | --- |
| **Asset Name** | **Threat Description** | **Vulnerability Description** |
| Electronic messaging software | Conectare neautorizata, Spionare, Cadere retea | Atac de retea, parole simple si slabe, lipsa unei copii de rezerva |
| Operating Sistem | Conectare neautorizata la porturi, Exploatarea punctelor slabe a SO, Atac de retea | SO vechi, configurare incompleta a routerului, lipsa unei copii de rezerva. |
| Server | Acces liber, introducerea virusilor, troienilor, exploatarea neautorizata, modificarea pachetelor de date | Permiterea accesării serverului de catre persoanele neautorizate (nonorganizationale), aplicatii netestate , lipsa configurarilor |
| Keyboard | Distrugerea echipamentului, tastelor | Acces liber la dispozitiv, acces la modificarea documentației |

### CONSECINȚE ȘI PROBABILITATEA

Odată ce riscurile au fost identificate, a fost necesar să evaluăm consecințele pentru fiecare combinație de amenințări și vulnerabilități pentru un activ individual:

|  |  |  |
| --- | --- | --- |
| Consecință joasă | 0 | Pierderea confidențialității, disponibilității sau integrității nu afectează fluxul de numerar al organizației, obligațiile legale sau contractuale sau reputația acesteia. |
| Consecință medie | 1 | Pierderea confidențialității, disponibilității sau integrității implică costuri și are un impact scăzut sau moderat asupra obligațiilor legale sau contractuale sau a reputației organizației. |
| Consecință înaltă | 2 | Pierderea confidențialității, disponibilității sau integrității are un impact considerabil și/sau imediat asupra fluxului de numerar, operațiunilor, obligațiilor legale sau contractuale ale organizației sau reputației acesteia. |

După evaluarea consecințelor, a fost necesar să evaluăm probabilitatea apariției unui risc, adică probabilitatea ca o amenințare a exploatat vulnerabilitatea activului respectiv:

|  |  |  |
| --- | --- | --- |
| Probabilitate joasă | 0 | Controalele de securitate existente sunt puternice și au oferit până acum un nivel adecvat de protecție. Nu sunt așteptate noi incidente în viitor. |
| Probabilitate medie | 1 | Controalele de securitate existente sunt moderate și au oferit în mare parte un nivel adecvat de protecție. Sunt posibile noi incidente, dar nu foarte probabile. |
| Probabilitate înaltă | 2 | Controalele de securitate existente sunt scăzute sau ineficiente. Astfel de incidente au o probabilitate mare de a avea loc în viitor. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name** | **Consequence** | **Probability** | **Threat Description** | **Vulnerability Description** |
| Electronic messaging software | 1 | 0 | Conectare neautorizata, Spionare, Cadere retea | Atac de retea, parole simple si slabe, lipsa unei copii de rezerva |
| Operating Sistem | 2 | 1 | Conectare neautorizata la porturi, Exploatarea punctelor slabe a SO, Atac de retea | SO vechi, configurare incompleta a routerului, lipsa unei copii de rezerva. |
| Server | 2 | 2 | Acces liber, introducerea virusilor, troienilor, exploatarea neautorizata, modificarea pachetelor de date | Permiterea accesării serverului de catre persoanele neautorizate (nonorganizationale), aplicatii netestate , lipsa configurarilor |
| Keyboard | 0 | 1 | Distrugerea echipamentului, tastelor | Acces liber la dispozitiv, acces la modificarea documentație. |

### TRATAREA RISCULUI ȘI PLANUL DE TRATARE A RISCULUI

Tratarea riscului este procesul de selectare și implementare a măsurilor de modificare a riscului. Măsurile de tratare a riscurilor au inclus evitarea, optimizarea, transferul sau păstrarea riscului. Măsurile de securitate au fost selectate din seturi de măsurători de securitate care sunt utilizate în cadrul Sistemului de Management al Securității Informaționale (SMSI) al băncii MAIB.

Având un tablou clar al riscurilor de securitate a informației sa elaborat Planul de tratare a riscului. Standardul ISO/IEC 27001:2013 stabilește următoarele variante de tratare a riscurilor:

* Diminuarea riscului – nivelul riscului urmează să fie redus prin aplicarea unor mijloace de control astfel, ca riscul rezidual să fie la un nivel acceptabil.
* Acceptarea riscului – acceptarea conștientă și obiectivă a riscului pentru a deschide o oportunitate cu condiția, că riscul nu este în contradicție cu politicile organizației și criteriile de acceptare a riscului.
* Evitarea riscului – renunțarea la activitățile sau condițiile care pot genera un risc.
* Transmiterea riscului – riscul se transmite unei terțe părți, care dispune de competențe mai înalte pentru controlul riscului.

La elaborarea planului de tratare a riscurilor au fost selectate și utilizate obiectivele de control şi măsurile de securitate conform ISO/IEC 27001:2013 (Anexa A) pentru a acoperi cerințele de securitate a informaţiei, inclusiv cele legale, de reglementare şi contractuale.

Măsurile încluse în Planul de Tratare sunt:

* instalarea unei camere wireless pentru monitorizare vizitatori din receptia băncii si instalarea unei linii telefonice ;
* informare sucursalelor băncii MAIB privind aceaste vulnerabilități;
* instruire personal privind procedurile de backup, utilizare a resurselor si de control aa accesului;
* instruire personal privind politica antivirus;
* instruire personal privind politica de utilizare a resurselor IT si politica de backup.

### DECLARAȚIA DE APLICABILITATE

Declarația de aplicabilitate (SoA) este principala legătură între evaluarea riscului și tratamentul risculul în întreprinderea, prin urmare, este o cerință pentru implementările sistemului de management al securității informațiilor (SMSI). SoA este un document actualizat și controlat continuu, care oferă o imagine de ansamblu asupra implementării securității informațiilor.

ISO 27001:2013 include declarație documentată (SoA) cu 35 de obiective de control și 114 controale cuprinzătoare de implementat într-un ISMS organizațional. SoA oferă un motiv pentru includerea sau excluderea oricăruia dintre controalele SoA în ISMS.

Procesul de producere a SoA și implementarea ISMS a constituit:

* Metoda sau procesul respectiv documentat.
* Procesele au conținut controale ca audituri și revizuiri.
* MAIB are scop de securitate, care este menționat în politica de securitate a informațiilor.
* Banca verifică și îmbunătățește continuu procesele și controalele.

Avantajele declarației de aplicabilitate este că explică succint controalele și este acceptabilă pentru auditorul care a evaluat întreprinderea. Primul pas către un SoA a fost o evaluare a riscului de securitate a informațiilor cu criterii de acceptare a riscurilor mapate. Procesul de evaluare a riscurilor a fost asociat cu pierderea confidențialității, integrității și disponibilității informațiilor, care trebuie să includă:

* Oameni
* Software
* Hardware
* Date și baze de date
* informație
* Istoricul atacurilor
* Audituri anterioare
* Controale curente și planificate pentru a reduce riscul
* Exercițiu extern de vulnerabilitate, evaluare și penetrare
* Experți în materie
* Proceduri sau instrucțiuni de lucru la care personalul trebuie să le respecte

SoA este documentul central pe care auditorii de securitate a informațiilor l-au folosit pentru a parcurge controalele procesului SMSI. SoA explică succint controalele de securitate a informațiilor care sunt relevante pentru întreprindere.

## VALABILITATEA ȘI MANAGEMENTUL DOCUMENTELOR

Acest document este valabil de la 11.11.2022.

Deținătorul acestui document este managerul pe securtiate, care va verifica și, dacă este necesar, va actualiza documentul cel puțin o dată pe an, înainte de revizuirea periodică a evaluării riscurilor existente.

Atunci când sa evaluat eficacitatea și caracterul adecvat al acestui document, au fost luate în considerare următoarele criterii:

* numărul de incidente care au avut loc, dar nu au fost incluse în evaluarea riscurilor
* numărul de riscuri care nu au fost tratate corespunzător
* numărul de erori în procesul de evaluare și tratare a riscurilor din cauza definirii neclare a rolurilor și responsabilităților