Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 1

# La disciplina „Managementul și Auditul Securitații Informaționale”

Tema: “[Evaluarea RI utilizind Microsoft Security Assessment ToolAssignment](https://else.fcim.utm.md/mod/assign/view.php?id=10820).”

A efectuat: st. gr. SI-211 A. Chihai

A verificat: E. Nemerenco

Chișinău – 2024

**Introducere**

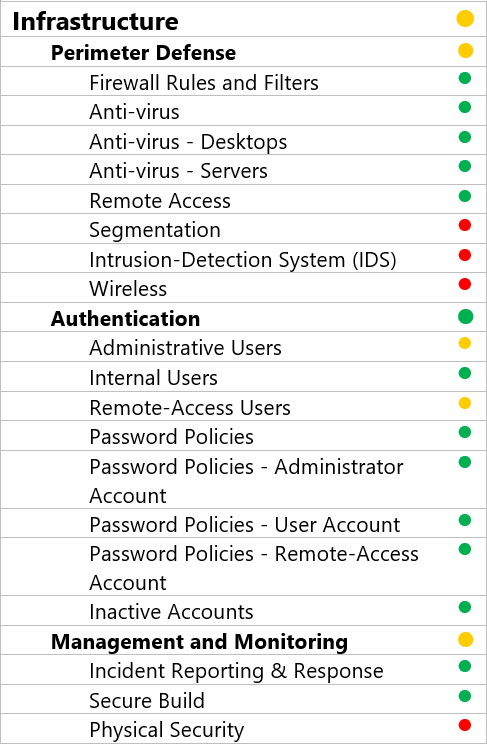
Mai jos este un raport care compară Profilul de Risc al Afacerii (Business Risk Profile - BRP) și Indicele de Apărare în Profunzime (Defence-in-Depth Index - DiDI) pentru o organizație. Se măsoară riscul de afaceri pe baza mediului de afaceri și a industriei prin BRP, în timp ce DiDI evaluează apărările de securitate folosite în diferite aspecte precum oameni, procese și tehnologie. Raportul subliniază importanța echilibrării acestor scoruri, indicând că disparitățile pot semnala necesitatea unui examen și ajustare suplimentară a strategiilor de securitate. De asemenea, accentuează semnificația considerării scorurilor BRP și DiDI în relație unul cu celălalt pentru o înțelegere cuprinzătoare a posturii de risc și securitate a unei organizații.

# Business Risk Profile vs. Defense-in-Depth Index Summary Report

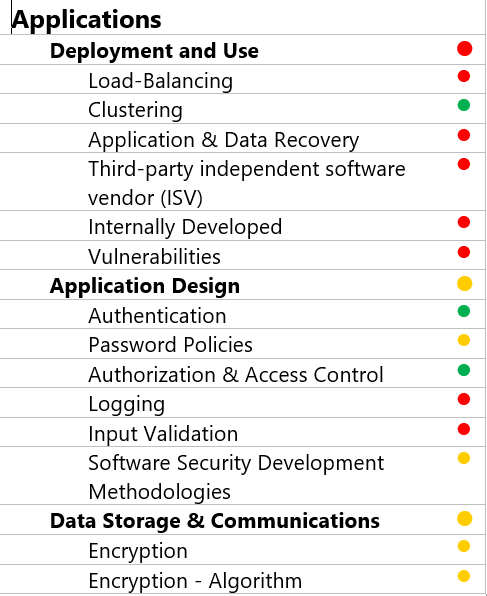
**BRP (Business Risk Profile)** variază de la 0 la 100, unde un scor mai mare implică o cantitate mai mare de risc potențial de afaceri pentru acel AoA (Articles of Association) specific. Este important de reținut că un scor de zero nu este posibil aici; desfășurarea afacerilor în sine implică un anumit nivel de risc. De asemenea, este important să înțelegeți că există unele aspecte ale conducerii unei afaceri care nu au o strategie directă de atenuare.

**DiDI** variază, de asemenea, de la 0 la 100. Un scor mare indică un mediu în care au fost luate un număr mai mare de măsuri pentru a implementa strategii de apărare în profunzime într-un anumit AoA. Scorul DiDI nu reflectă eficacitatea generală a securității sau chiar resursele cheltuite pentru securitate, ci mai degrabă este o reflectare a strategiei generale utilizate pentru apărarea mediului.

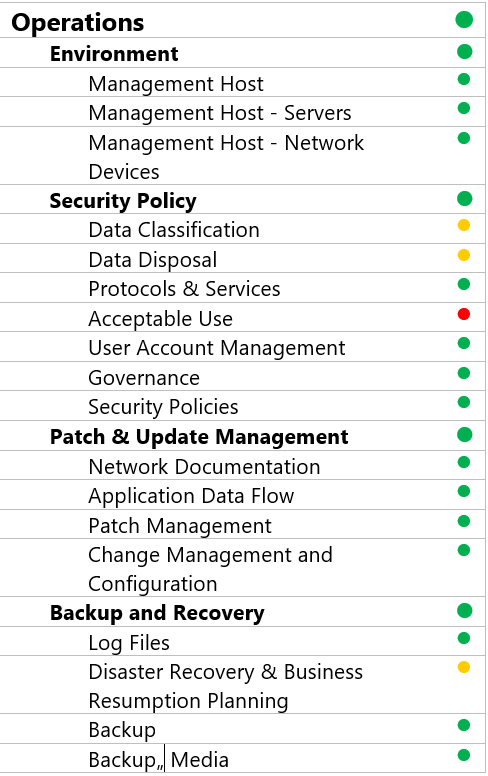
|  |  |  |
| --- | --- | --- |
| **Areas of Analysis** | Risk-Defense Distribution | Security Maturity |
| **Infrastructure** | **** | **** |
| **Applications** | **** | **** |
| **Operations** | **** | **** |
| **People** | **** | **** |

****

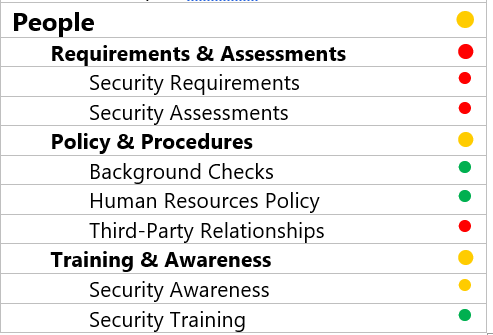
Din poza de mai sus putem vedea vulnerabilitățile infrastructurii, care sunt în mare parte bune, doar ca avem nevoie de dezvoltare anumitor domenii cum ar fi rețeaua wireless si securitatea fizică.



Aplicațiile utilizate în cadrul companiei au un rol mare în ce ține cont de Securitate. Ne putem da seama din tabel că nivelul de vulnerabilitate e unul destul de ridicat, vor fi nevoie de luat măsuri pentru a preveni unele atacuri posibile și de rezolvat. Aplicațiile fiind un canal de comunicare cu furnizorii terți și periculoase.



Operțiunile sunt acțiuni directe atât ale personalului, cât și angajaților întreprinderii. Din tabelul de mai sus se poate deduce că aceste operațiuni sunt destul de securizate, iar datele sunt salvate și realizate copii de rezervă ale lor.



Personalul are un nivel alarmant de cunoștințe în securitate și sunt pasibili la atacurile potențiale, astfel ar pune și compania la un risc posibil, daca ar accesa un email sau nu ar ști cum să identifice aceste amenințări.

**Concluzie**

În concluzie, evaluarea Riscului de Afaceri (BRP) și Indicele de Apărare în Profunzime (DiDI) pentru organizația analizată evidențiază aspecte semnificative ale securității informaționale. Discrepanțele dintre BRP și DiDI subliniază necesitatea unei atenții continue asupra strategiilor de securitate pentru a asigura o echilibrare corespunzătoare între riscurile potențiale și măsurile de apărare implementate. Îmbunătățirea infrastructurii, gestionarea eficientă a vulnerabilităților din aplicații și consolidarea cunoștințelor personalului în domeniul securității reprezintă aspecte critice pentru întărirea poziției organizației în fața amenințărilor cibernetice. Este esențială adoptarea unei abordări proactive pentru identificarea și gestionarea riscurilor, asigurând astfel securitatea informațională și continuarea operațiunilor într-un mediu sigur.