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 S. Chirita

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

## Interpreting the Graphs

* BRP ranges from 0 to 100, where a higher score implies a greater amount of potential business risk for that specific AoA. It is important to note that a score of zero is not possible here; conducting business in itself implies some level of risk. It is also important to understand that there are some aspects of running a business that have no direct mitigation strategy.
  + **Business Risk Profile (BRP)** - A measurement of the risk to which an organization is exposed, based on the business environment and industry in which it competes.
  + **AoAs** - Areas of Analysis which are infrastructure, applications, operations, and people.
* DiDI also ranges from 0 to 100. A high score indicates an environment where a greater number of measures have been taken to deploy defense-in-depth strategies in a particular AoA. The DiDI score does not reflect overall security efficacy or even resources spent on security, rather it is a reflection of the overall strategy used to defend the environment.
  + **Defence-in-Depth Index (DiDI)** - A measurement of the security defences used across people, process and technology to help to mitigate the risks identified for a business.

Intuitively, it may seem that a low BRP score and a high DiDI score are a good outcome, but this is not always the case. The scope of this self-assessment does not allow for all factors to be taken into consideration. Significant disparity between BRP and DiDI scores in a particular AoA suggests that further examination of this AoA is recommended. When analyzing your results it is important to consider the individual scores, both BRP and DiDI, in relation to one another. A stable environment will probably be represented by relatively equal scores across all areas.

Disparities between DiDI scores are a strong indicator that overall security strategy is focused on a single mitigation technique. If the security strategy does not balance people, process and technology aspects, the environment will probably be more vulnerable to attack.

**Rezumat**

Am analizat raportul detaliat privind evaluarea securității pentru Alah\_Abar SRL. Rezumatul subliniază aspectele critice și recomandările în patru domenii principale: Infrastructură, Aplicații, Operațiuni și Oameni.

**Infrastructură**: Se recomandă îmbunătățirea apărării perimetrale, a măsurilor antivirus și a protocoalelor de acces la distanță. Printre sugestii se numără segmentarea rețelei, sisteme avansate de detectare a intruziunilor și protocoale robuste de securitate wireless.

**Aplicații**: Raportul sugerează asigurarea securității aplicațiilor prin actualizări regulate, adoptarea metodologiilor de dezvoltare sigure și îmbunătățirea designului aplicațiilor pentru a include autentificare și controluri de acces mai puternice.

**Operațiuni**: Recomandările cheie includ implementarea unor politici de securitate stricte, îmbunătățirea clasificării și procedurilor de eliminare a datelor, precum și îmbunătățirea gestionării actualizărilor și patch-urilor. De asemenea, se subliniază importanța planificării recuperării după dezastre și reluarea afacerii.

**Oameni**: Accentul este pus pe întărirea formării și conștientizării securității, efectuarea regulată a evaluărilor de securitate și stabilirea unor politici și proceduri clare pentru resurse umane și relații cu terți.

**Puncte Tari:**

*Tehnologie Avansată:* Utilizarea tehnologiilor de securitate avansate, cum ar fi firewall-uri, antivirusuri și sisteme de prevenire a intruziunilor.

*Politici Stricte de Securitate:* Existenta unor politici clare și bine implementate privind securitatea IT.

*Conștientizarea Angajaților:* Nivel ridicat de conștientizare a securității în rândul angajaților.

*Managementul Riscurilor:* Abordare proactivă în identificarea și gestionarea riscurilor de securitate.

**Puncte Slabe:**

*Lipsa Formării Periodice*: Insuficienta formare a personalului în privința amenințărilor de securitate și a celor mai bune practici.

*Vulnerabilități în Aplicații și Dispozitive:* Prezența vulnerabilităților nerezolvate în software și hardware.

*Securitate Fizică Inadecvată:* Protecția fizică insuficientă a infrastructurii IT.

*Planificare Insuficientă pentru Continuitatea Afacerii:* Lipsa unor planuri robuste pentru recuperarea după incidente majore de securitate.