Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 3

# La disciplina „Managementul și Auditul Securitații Informaționale”

Tema: “Estimarea timpului de implementare a SMSI conform ISO 27001 / ISO 22301 și GDPR”

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

A verificat: E. Nemerenco

Chișinău – 2024

**ISO 27001**

Calculatorul de timp pentru ISO 27001 oferă o estimare a timpului necesar pentru implementarea standardului ISO 27001:2013 în funcție de diferiți factori specifici organizației. Acești factori includ numărul de angajați, departamente și locații fizice, implementarea altor standarde sau regulamente, utilizarea consultanței și a expertizei interne sau externe, utilizarea șabloanelor de documentație, existența unui coordonator pentru proiect și susținerea managementului superior. Pe baza acestor informații, calculatorul oferă o estimare a timpului necesar pentru implementare.

**Înțelegerea Implementării ISO 27001: Întrebări cheie și Rezultate**

Thank you for using our Calculator!

To have a better understanding of your results, try our online ISO 27001:2013 Foundations Course <http://bit.ly/iso27001foundations-idc>

Here's the information you have filled in:

Q. Number of employees

R. 1 to 20

Q. Number of departments

R. 1 to 3

Q. Number of physical locations

R. 1

Q. Have you already implemented some other standard like PCI DSS, ITIL, ISO 9001, or similar?

R. We're just starting to implement it.

Q. Are you going to use a consultant or some other in-house or external ISO 27001/ISO 22301 expert?

R. Yes, for the whole project.

Q. Do you have an employee who will coordinate and manage this project?

R. Yes, a person with little experience in managing projects whenever he/she finds free time.

Q. Do you have support from your senior management for this project?

R. Nominally yes, but management doesn't understand they'll have to participate and invest resources.

Q. Estimated number of months required for implementation:

R. 9

Scopul acestor întrebări a fost de a obține informații despre dimensiunea companiei, numărul de angajați și nivelul sau dacă sunt implementate alte standarde utilizate cum ar fi PCI DSS, ISO 9001… . Alt lucru de care ține cont acest formular este dacă avem un consultant care va ajuta pe pracurs pentru implementarea ISO 27001/ISO 22301.

**GDPR**

Aceste întrebări sunt concepute pentru a colecta informații relevante despre prelucrarea datelor personale în cadrul organizației. Ele vizează diferite aspecte ale procesării datelor personale, inclusiv dimensiunea organizației, tipurile de date personale prelucrate, rolurile de controller și processor, practicile de profilare și luarea deciziilor automate, utilizarea terților pentru procesarea datelor, implementarea standardelor de securitate și sprijinul din partea managementului superior.

Informațiile colectate prin aceste întrebări sunt esențiale pentru evaluarea nivelului de conformitate cu GDPR și pentru a determina efortul și timpul necesar pentru implementarea măsurilor necesare. După completarea acestor întrebări, veți primi rezultatele estimării, iar dacă doriți, acestea pot fi trimise către dvs. prin e-mail pentru o referință ulterioară.

Thank you for using our Calculator!

Here's the information you have filled in:

Q. Number of employees

R. 1 to 20

Q. Categories of personal data processed

R. Personal data such as name, surname, email address, telephone number, IPs, mobile device IDs, location data, an online identifier, etc.

Q. Are you mainly acting as a data controller or a data processor?

R. Both data controller and data processor

Q. Do you engage in profiling and/or automated decision-making\*?(\*Profiling means any form of automated processing consisting of the use of personal data to evaluate an individual, in particular to analyse or predict aspectsconcerning that individual 's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Automated decision-making means you are making decisions concerning the individuals without any human involvement such as automated credit scoring.)

R. Profiling

Q. Do you have any subsidiaries outside the EU?

R. No

Q. Do you use third parties (processors) that are processing personal data on your behalf, such as payroll providers, call centres, or security companies?

R. No

Q. Have you already implemented a security standard like ISO 27001, COBIT, NIST Cybersecurity Framework, or similar?

R. We're just starting to implement it.

Q. Are you going to use a consultant or some other in-house or external GDPR expert?

R. Only for parts of the project

Q. Are you going to use documentation templates for your policies, procedures, plans, forms, etc.?

R. Only for some of the documents

Q. Do you have an employee who will coordinate and manage this project?

R. Yes, a person with experience in project management; however, he/she is quite busy.

Q. Do you have support from your senior management for this project?

R. Yes, management has clear objectives and is aware of all the commitments required.

Q. Estimated number of months required for implementation:

R. 6

Q. Enter your email if you want these results to be sent to you:

R. [adrian.chihai@isa.utm.md](mailto:stanislav.chirita@isa.utm.md)

Aceste informații sunt fundamentale pentru evaluarea nivelului de conformitate cu reglementările privind protecția datelor și pentru determinarea efortului și timpului necesar pentru implementarea măsurilor corespunzătoare. După completarea acestor întrebări, veți primi rezultatele estimării, iar dacă doriți, acestea pot fi trimise către dvs. prin e-mail pentru o referință ulterioară.

**Concluzie**

În urma completării acestor seturi de întrebări, puteți obține o imagine clară asupra nivelului de pregătire și necesitatea implementării standardelor de securitate și a conformității cu reglementările privind protecția datelor în organizația dvs. Informațiile colectate vizează aspecte esențiale precum dimensiunea și structura organizației, tipurile de date personale prelucrate, practicile existente și sprijinul din partea managementului superior. Acestea vă vor ajuta să identificați zonele de vulnerabilitate și să determinați efortul și timpul necesar pentru implementarea măsurilor corespunzătoare. În final, obiectivul este să vă asigurați că organizația dvs. este pregătită să gestioneze și să protejeze în mod eficient datele personale, respectând reglementările aplicabile și îndeplinind așteptările clienților și partenerilor de afaceri.