Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

**Raport la**

**Lucrarea de laborator Nr.4**

*Disciplina: Managementul și Auditul Securității Informaționale*

**Tema: ” Evaluarea conformității sistemului de securitate informațională cu recomandările ISO 27001 si GDPR .** **Domeniile ISO 27001.”**

A efectuat: st. grp. SI-201: Cebotari Dan

A verificat: asist.univ. Cunev Igor

Chișinău – 2022

**Scopul lucrării:**

Evaluarea cerințelor standardului de securitate utilizând Free ISO 27001 Gap Analysis Tool și EU GDPR Readiness Assessment Tool. Familiarizarea şi studierea sistemului informaţional DS CONDOR. Declarația de aplicabilitate.

**Sarcina lucrării:**

Studierea și utilizarea instrumentelor Free ISO 27001 Gap Analysis Tool și EU GDPR Readiness Assessment Tool.

**Studierea și utilizarea sistemului informaţional DS CONDOR.**

Certificarea si implementarea unui ***SMSI*** reprezinta o decizie strategica pentru orice tip de organizatie deoarece acesta garanteaza securitatea informatiilor ale societatii certificate si a informatiilor partenerilor de afaceri si a clientilor.

Acest sistem ofera recomandari pentru pastrarea sub control al tuturor riscurilor informationale, aducand o clarificare asupra tuturor tipurilor de amenintari si ofera directii de tratare ale metodelor de protectie pentru asigurarea supravietuirii companiei, minimizarea daunelor financiare si apoi mixamizarea perspectivelor organizatiei dar si a intregului profit.

***Gap Analysis***

Analiza decalajului este opțiunea simplă, în această analiză trebuie doar să luăm o listă de „cerințe” și să determinăm dacă am implementat fiecare dintre elementele de pe listă.

De exemplu, putem lua toate controalele enumerate în Anexa A a ISO 27001 și apoi să le verificăm dacă le-am implementat pe fiecare în companie. Acolo unde un control nu este implementat, există un „decalaj”. Apoi, putem lua măsuri pentru a aborda acest decalaj prin implementarea controlului.

În ceea ce privește avantajele și dezavantajele efectuării unei analize a decalajelor, marele beneficiu este că este mai rapid și mai puțin costisitor de efectuat în comparație cu o evaluare a riscurilor.

Dezavantajul este că nu putem determina neapărat dacă trebuie să implementăm fiecare dintre controalele enumerate – unele dintre ele pot fi costisitoare de implementat și consumatoare de timp pentru a opera.

**Utilizarea instrumentului Free ISO 27001 Gap Analysis Tool**

Implementarea sistemului de management pentru securitatea informatiei şi certificarea ISO 27001 a companiei demonstrează angajamentul pentru protecţia datelor procesate, continuitatea activităţilor (business continuity) şi respectarea legislaţiei naţionale şi internaţionale în domeniu.

Etapele implementării certificarii SMSI ISO 27001(securitatea informatiei):

* Evaluarea riscului şi impactului incidentelor grave asupra firmei
* Tratarea riscurilor respectand cerinţele standardelor utilizate ca referinţă pentru Sistemele de management ale securitatii informatiilor.

**O analiză a decalajelor ISO 27001** oferă o imagine de ansamblu la nivel înalt a ceea ce trebuie făcut pentru a obține certificarea și ne permite să evaluam și să comparam aranjamentele existente de securitate a informațiilor ale organizației cu cerințele ISO 27001.

Este soluția ideală pentru organizațiile care trebuie să își măsoare starea actuală de conformitate cu Standardul și permite să definim parametrii ISMS în toate funcțiile de afaceri.

Realizat de un specialist ISO 27001, acest serviciu vă va oferi o evaluare informată a:

* Lacunele de conformitate;
* Domeniul de aplicare propus pentru ISMS;
* Cerințele de resurse interne;
* Termenul potențial pentru obținerea pregătirii pentru certificare.

Standardul ISO 27001 a fost dezvoltat pentru a oferi un model consistent pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui Sistem de management al securității informațiilor (ISMS). ISMS nu este un sistem universal. Mai degrabă, proiectarea, implementarea, monitorizarea și întreținerea ISMS al unei organizații ar trebui să se bazeze pe nevoile și cerințele unice ale acestora

|  |  |
| --- | --- |
| **ISO 27001 - PDCA** | |
| **Planifică** | Stabilirea politicii, obiectivelor, proceselor și procedurilor ISMS relevante pentru gestionarea riscurilor și îmbunătățirea securității informațiilor pentru a oferi rezultate în conformitate cu politicile și obiectivele generale ale unei organizații. |
| **Efectuează** | Implementarea și operațiunea cu politica, controalele, procesele și procedurile ISMS. |
| **Verifică** | Evaluarea și măsurarea performanței procesului în raport cu politica, obiectivele și experiența practică ISMS și raportarea rezultatele conducerii pentru revizuire. |
| **Acționează** | Luarea acțiunilor corective și preventive, pe baza rezultatelor auditului intern ISMS și revizuirea managementului sau a altor informații relevante, pentru a obține îmbunătățirea continuă a ISMS. |



Figura 1 – Rezultatele utilizării instrumentului

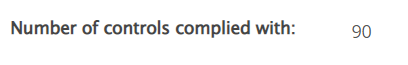


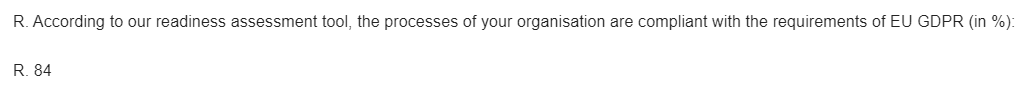
Figura 2 – Rezultatele utilizării instrumentului

**Utilizarea instrumentului EU GDPR Readiness Assessment Tool**

GDPR al UE : responsabilitatea legală pentru prelucrarea legală a datelor cu caracter personal revine proprietarilor și operatorilor site-ului web.

Tehnologiile necesare pentru a îndeplini cerințele GDPR trebuie să fie tehnologii care sunt implementate de proprietarii site-ului web, nu de utilizatori – software GDPR care se aplică schimbărilor structurale pe care le creează GDPR, nu soluții de autoapărare pentru fiecare utilizator individual de acolo.

|  |  |
| --- | --- |
| **Evaluarea gradului de pregătire GDPR** | |
| **CINE** | Întreprinderi care oferă bunuri sau servicii (indiferent dacă este necesară plata) în UE, precum și întreprinderi care monitorizează comportamentul subiecților UE în UE. |
| **CE** | Au fost emise noi mandate de confidențialitate a datelor prin regulamentul Uniunii Europene |
| **UNDE** | Include orice organizație din lume dacă reține sau prelucrează informații despre orice cetățean din UE. |
| **DE CE** | Pentru a proteja mai bine informațiile personale ale oricărui individ, pentru a asigura drepturile persoanei asupra informațiilor colectate și pentru a forța întreprinderile să urmeze o schemă uniformă de protecție a datelor. |



**Figura 3** – Rezultatele utilizării instrumentului

***ISO 27001 Gap Analysis vs EU GDPR Readiness Assessment Tool***

|  |  |  |
| --- | --- | --- |
|  | **ISO 27001 Gap Analysis** | **EU GDPR Readiness Assessment Tool** |
| **Despre** | Este o evaluare care oferă o imagine de ansamblu la nivel înalt asupra poziției actuale de securitate a organizației;  Analiza decalajului măsoară starea actuală de conformitate cu standardul și, de asemenea, vizează parametrii ISMS ai organizației în toate funcțiile de afaceri | Ajută să identifica starea actuală de conformitate cu GDPR a organizației; instrumentul segmentează GDPR în teme viabile și conduce print-o serioe de intrebări legată de fiecare temă |
| **Beneficii** | Analiza decalajului vizează parametrii ISMS în toate funcțiile de afaceri.  Analiza oferă claritate cu privire la ceea ce trebuie inclus în domeniul de aplicare al ISMS și controalele care trebuie implementate. | Oferă un instantaneu precis al pregătirii organizației pentru a se conforma cu GDPR UE.  Analizează amănunțit nivelul la care se afla acum organizația și starea riscurilor actuale. |
| **Componente** | Acesta detaliază postura de securitate pentru fiecare dintre cele 114 controale de securitate a informațiilor care sunt prezentate în **Anexa A** a ISO 27001.  De asemenea mai conține 7 capitole, pentru o analiză mai aprofundată. | GDPR este împărțit în 6 capitole și 32 de întrebări. |

**Utilizarea sistemului informaţional DS CONDOR.**

**CONDOR** este un sistem puternic de dezvoltare și gestionare a politicii de securitate a informațiilor a unei companii bazat pe standardul ISO 17799, ISO 27001. CONDOR este un instrument modern pentru dezvoltarea tuturor prevederilor principale ale politicii de securitate a informațiilor a companiei dumneavoastră și gestionarea procesului de implementare a acestor prevederi în practică.

**Sistemul CONDOR**

* Identifică toate punctele slabe ale politicii de securitate a sistemului de informații.
* Analizează riscul de nerespectare a fiecărei prevederi a politicii de securitate și le ierarhizează în funcție de gradul de criticitate, ceea ce oferă posibilitatea de a prioritiza acțiunile planificate.
* Permite gestionarea eficientă a riscurile care decurg din nerespectarea prevederilor politicii de securitate.

Aspectele managementului securității informațiilor precum:

* politică de securitate;
* metode organizatorice pentru asigurarea securității informațiilor;
* managementul resurselor;
* utilizatorii sistemului informatic;
* siguranță fizică;
* comunicarea si managementul proceselor;
* controlul accesului;
* achizitia, dezvoltarea si intretinerea sistemelor informatice;
* managementul incidentelor de securitate a informațiilor;
* Managementul continuității activității;
* conformitatea sistemului cu cerințele.

Sistemul CONDOR este alcatuit din aproape toate prevederile standardului ISO 17799 și ISO 27001, formulate sub forma de intrebari, prin care odată răspunse obținem o imagine completa - ce prevederi din sistemul sunt indeplinite si care nu. Fiecare prevedere a standardului are o pondere implicită care caracterizează gradul de criticitate al acestei prevederi pentru a menține nivelul necesar de securitate.

**Declarația de aplicabilitate**

**Declaratie de aplicabilitate** (definitie ISO 27001 pentru securitatea informatiei) este un document care expune obiectivele de control si masurile de control legate de securitatea informatiei din organizatie.

Pentru a ne da seama despre care ar trebui sa fie obiectivele de control si masurile de control legate de securitatea informatiei proprii numai organizatiei , trebuie sa efectuăm o apreciere a riscului, sa alegem tratamente ale riscului, sa identificăm toate cerintele legale si de reglementare relevante, sa studiem obligatiile contractuale si sa analizăm nevoile si cerintele organizatiei.

|  |  |
| --- | --- |
| **Declarația de aplicabilitate (ISO 27001)** | |
| **Despre** | Maparea măsurilor de securitate implemetate pe cele din Anexa A, ISO/IEC 27001;  Menționarea excepțiilor, argumentarea neselecției, măsurile compensatorii;  Poate fi utilă pentru eficientizarea controalelor BNM. |
| **Stabilește** | probabilitatea reziduală de apariție;  gravitatea reziduală a impactului;  nivelul riscului rezidual; |
| **Conținut** | Anexa A din ISO/IEC 27001;  Pot fi utilizate unele din cele 114 măsuri propuse din anexă, căci unele din acestea pot fi declarate neaplicabile. |

|  |  |
| --- | --- |
| **Declarația de aplicabilitate (GDPR)** | |
| **Despre** | **Cerințele Regulamentului(UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice, în legătură cu prelucrarea datelor cu caracter personal și libera circulație a acestor date, și de abrogare a Directivei     95/46/CE (Regulamentul General privind Protecția Datelor)** |
| **Stabilește** | Utilizarea pseudonimizării și criptarea datelor cu caracter personal;  Asigurarea unei credibilități permanente, a integrității și disponibilității sistemelor informatice pe care le utilizăm cu scopul de a presta servicii pentru societate  Capacitatea, prin măsuri adecvate, de a răspunde unei cereri de exercitare a drepturilor de către un subiect de date cu caracter personal (Capitolul III din RGPD); |
| **Conținut** | Cele 6 capitole și 32 de subiecte |

**Concluzie:**

Astfel fiecare călătorie de confidențialitate are nevoie de un punct de plecare. Doar dacă știi unde te afli, devine clar ce măsuri sunt necesare.

Auditul intern și îmbunătățirea continuă sunt esențiale pentru menținerea unui sistem efficient sistem de management; trebuie dezvoltat un program de audit intern şi implementate și neconformitățile identificate din audituri și din alte domenii ar trebui să fie introduse în procesul de îmbunătățire.

În timpul unei evaluări (sau auditului oficial), este testat temeinic în ce măsură organizația îndeplinește cerințele. O analiză amănunțită oferă o perspectivă clară și, de asemenea, expune imediat punctele de atenție

Gap Analysis ajută companiile să înțeleagă cea mai bună modalitate de a-și îmbunătăți și eficientiza sistemele interne de management al securității informațiilor pentru a se asigura că îndeplinesc cerințele standardelor analizate în această lucrare.

În urma lucrului cu sistemul CONDOR, primim un raport care conține toate prevederile standardului ISO 17799 și ISO 27001 îndeplinite și neîndeplinite în compania, o analiză a eficienței implementării prevederilor restante și comentarii ale experților. Sistemul conține mostre și formulare de documente pentru implementarea prevederilor politicii de securitate.