Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

**Raport la**

**Lucrarea de laborator Nr.3**

Disciplina: Managementul și Auditul Securității Informaționale

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

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

A verificat: asist. univ. : Cunev Igor

Chișinău – 2022

**Scopul lucrării:**

Estimarea timpului de implementare a SMSI conform ISO 27001 / ISO 22301 și GDPR.

**Sarcina lucrării:**

Studierea și utilizarea instrumentelor ISO 27001 / ISO 22301 Implementation Duration și EU GDPR Compliance Duration Calculator.

**Utilizarea istrumentului ISO 27001 / ISO 22301 Implementation Duration Calculator**

Acest calculator ajută la estimarea timpului necesar pentru implementarea ISO 27001 sau ISO 223021. După răspunderea la întrebările propuse de site-ul <https://advisera.com/27001academy/free-tools/free-calculator-duration-of-iso-27001-iso-22301-implementation/> , am primit timpul necesar de implementare a ISO 27001 sau ISO 223021 care este de 7 luni.

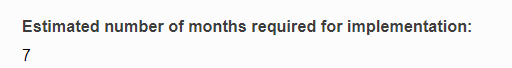


Figura 1 – Timpul necesar pentru implementarea ISO 27001 sau ISO 22301

**Procesul de certificare ISO 27001** include mai multe etape și fiecare implică un angajament de timp. Fiecare pas variază foarte mult, la fel ca și timpul pe care trebuie să-l facă echipele interne ale companiei .

**Stadiul de pregătire – 6 până la 10 luni**

Etapa de pregătire este cea mai lungă și cea mai intensă forță de muncă pentru echipele interne ale unei companii.

În această etapă a procesului de certificare, e nevoie de a numi o echipă de implementare, de a stabili sfera și obiectivele sistemului de management al securității informațiilor (ISMS) și de a dezvolta un plan de implementare.

**Etapa 1 Auditul documentației – 1 zi**

Auditul documentației în sine este de obicei rapid și finalizat într-o zi. Acest pas nu necesită eforturi grele din partea echipelor, dar acestea ar trebui să fie disponibile dacă auditorul are întrebări.

**Etapa 2 Audit de certificare – 6-10 zile**

În timpul etapei a doua a auditului, auditorul face o vizită. Ei stau la locația fizică a companiei pentru a vă evalua operațiunile și pentru a discuta cu echipa. Ca parte a auditului la fața locului, auditorii vor examinează ISMS, cerințele pentru clauzele patru până la 10, controalele din anexa A și dovezile tehnice asociate acestor controale.

**Remedierea neconformităților – Până la 6 luni**

Dacă auditorul decide că compania a îndeplinit toate cerințele ISO 27001, se va trece la etapa a doua a auditului de certificare.

Potrivit unui consultant de risc cibernetic, neconformitățile minore apar în 50% până la 75% din timp.

**Accelerarea cronologiei de audit a instrumentului ISO 27001**

Mulți factori pot afecta termenele pentru certificarea ISO 27001. De exemplu, cu cât organizația este mai mare și cu cât există mai multe locații fizice, cu atât procesul va dura mai mult.

Inițiativele de conformitate care sunt conduse în principal de angajații de la niveluri inferioare pot dura de două ori mai mult pentru a fi finalizate. Pentru a aduce echipa executivă la bord, ei trebuie informați despre obiectivele certificării și beneficiile pe care aceasta le oferă organizației;

* Un campion al proiectului

O inițiativă ISO 27001 delegată mai multor angajați pe o bază ad-hoc poate dura de două ori mai mult decât una pe care un singur angajat cu experiență o conduce strategic. Pentru a accelera procesul de certificare,este nevoie de a numi un lider de proiect cu experiență în managementul proiectelor;

* Software de conformitate

Automatizarea scurtează intervalele de timp, oferind un limbaj preîncărcat, cu cele mai bune practici, politici de domeniu și alt conținut de conformitate. Utilizarea instrumentelor salvează echipa internă de a începe de la zero și de a aborda un proiect de bricolaj. O platformă automatizează, de asemenea, sarcinile de colectare a dovezilor care necesită multă muncă și menține echipele pe drumul cel bun prin emiterea de mementouri automate pentru riscuri neabordate. Software-ul de conformitate reduce, de asemenea, marja de eroare și reduce șansele de neconformități.

De fapt, datele arată că utilizarea Tugboat Logic reduce timpul de conformitate cu până la 50%.

**ISO 22301** este standardul de management al continuității afacerii (BCM) dezvoltat de Organizația Internațională de Standardizare (ISO). Standardul stabilește un cadru pe care organizațiile îl pot adopta pentru a se pregăti mai bine, a preveni și a dezvolta protocoale în cazul unui dezastru.

Multe industrii solicită organizațiilor să le arate clienților și părților interesate că le pot furniza în mod continuu servicii de nivel premium. Aceasta include stocarea copiilor de rezervă ale datelor critice și luarea de măsuri pentru a minimiza pierderea în cazul unui dezastru, natural sau de altă natură.

**Utilizarea istrumentului** **EU GDPR CDC**

Acest calculator ajută la estimarea timpului necesar pentru implementarea EU GDPR . După răspunderea la întrebările propuse de site-ul <https://advisera.com/eugdpracademy/eu-gdpr-compliance-duration-calculator/> , am primit timpul necesar de implementare a EU GDPR care este de 11 luni.

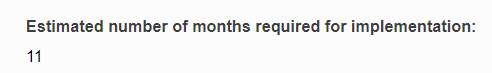


Figura 2 – Timpul necesar pentru implementarea EU GDPR

Regulamentul general privind protecția datelor (GDPR) este o legislație care a actualizat și unificat legile privind confidențialitatea datelor în Uniunea Europeană (UE).

**GDPR** se aplică dacă:

* compania prelucrează date cu caracter personal și are sediul în UE, indiferent de locul în care are loc prelucrarea reală a datelor;
* compania este stabilită în afara UE, dar prelucrează date cu caracter personal în legătură cu oferta de bunuri sau servicii către persoane fizice din UE sau monitorizează comportamentul persoanelor din UE.

Scopul GDPR este de a proteja persoanele și datele care le descriu și de a se asigura că organizațiile care colectează acele date fac acest lucru într-un mod responsabil. GDPR prevede, de asemenea, ca datele cu caracter personal să fie păstrate în siguranță; în parte, regulamentul spune că datele cu caracter personal trebuie protejate împotriva „prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorarii accidentale”

**ISO 27001 vs EU GDPR**

|  |  |  |
| --- | --- | --- |
|  | **ISO 27001** | **EU GDPR** |
| **Cerințe critice** | * Gestionarea activelor * Securitate operațională * Controlul accesului * Managementul incidentelor de securitate a informațiilor * Securitatea resurselor umane * Continuitatea afacerii | * Domeniu mai larg de date care necesită protecție * Consimțământul explicit * Drepturi extinse ale persoanelor vizate * Amenzi uriașe pentru nerespectare * Reguli stricte de notificare a încălcării datelor |
| **Necesitate** | ISO 27001 este o certificare voluntară care cere organizațiilor să adopte o abordare bazată pe riscuri a modului în care gestionează datele sensibile. | GDPR își propune să protejeze datele cu caracter personal ale cetățenilor UE, iar conformitatea cu GDPR este obligatorie pentru majoritatea organizațiilor care lucrează în Europa sau cu cetățenii UE. |

**Asemănări**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Confidențialitatea, disponibilitatea și integritatea datelor** | **Evaluare a riscurilor** | **Managementul furnizorilor** |
| **ISO 27001** | | **Clauza 4** cere organizațiilor să identifice problemele interne și externe care le-ar putea afecta programele de securitate. | ISO 27001 sfătuiește, de asemenea, organizațiile să efectueze o evaluare riscurilor pentru a identifica amenințările. | **Clauza 8** cere organizațiilor să identifice care acțiuni de procesare sunt externalizate și să se asigure că sunt capabile să țină acele acțiuni sub control. |
| **EU GDPR** | | **Articolul 5** specifică principiile generale pentru prelucrarea datelor, cum ar fi protecția împotriva „prelucrării neautorizate sau ilegale” | **Articolul 35** impune companiilor să efectueze evaluări de impact asupra protecției datelor pentru a evalua și identifica riscurile | **Articolul 28** cere operatorilor de date să asigure termenii contractuali și asigurări de la procesatorii, creând un „acord de prelucrare a datelor”. |

**Concluzie:**

În urma elaborării lucrării de laborator nr.3 am determinat timpul de implementarea SMSI conform ISO 27001 / ISO 22301 și EU GDPR. Astfel răspunzând la întrebările propuse de paginile web a calculatorul, a fost estimat timpul de implementare. Cu toate acestea pentru a înțelege de ce anume am primit un astfel de răspuns, a fost nevoie de o analiză amănunțită a acestor două instrumente. Instrumentul ISO 27001 necesită mult timp, dar certificarea sporește prestigiul companiei la nivel global. În plus, ajută la atragerea unui nou nivel de clienți de profil înalt și construirea încrederii. Înțelegând termenele implicate pentru fiecare etapă și știind cum să accelerăm procesul, putem minimiza întârzierile. Iar scopul GDPR este de a proteja persoanele și datele care le descriu și de a se asigura că organizațiile care colectează acele date fac acest lucru într-un mod responsabil. După o analiza a acestor două instrumente, pot spune că GDPR se concentrează pe confidențialitatea datelor și protecția informațiilor personale; cere organizațiilor să depună mai multe eforturi pentru a obține consimțământul explicit pentru colectarea datelor și pentru a se asigura că toate datele sunt procesate în mod legal.