Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

**Raport**

la Managementul și Auditul Securității Informaționale

Tema: „Comparația metodologiei Microsoft și a standardelor ISO 27005, NIST-SP-800-30 Nr.53 de evaluare a riscurilor informației”

Efectuat: st.gr. SI-201 Cebotari Dan,

st.gr. SI-201 Roman Nicoleta

A verificat: lect.univ. Bulai Rodica

Chișinău 2022

**5 asemănări și deosebiri**

27005 ISO / Metodologia Microsoft / NIST-SP-800-30 Nr. 53

**Asemanari**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteriu** | **Standardul**  **ISO 27005** | **Metodologia Microsoft** | **Standardul NIST-SP-800-30 Nr.53** |
| Analiza riscurilor | - Stabilirea contextului  - Evaluarea riscurilor  - Tratarea riscurilor  - Evitarea riscului  - Monitorizarea riscului  - Implementarea unui control  - Comunicarea riscurilor  - Consultarea riscurilor  - Revizuirea riscului | | |
| Tratarea riscurilor | - asumarea sau creșterea riscului pentru a urmări o oportunitate;  - eliminarea sursei de risc;  - schimbarea probabilității;  - modificarea consecințelor;  - împărțirea riscului cu o altă parte sau cu alte părți (inclusiv contracte și finanțarea riscului); și  - reținerea riscului printr-o alegere în cunoștință de cauză. | | |

**Nivelul de evaluare a riscului**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteriu** | **Standardul**  **ISO 27005** | **Metodologia Microsoft** | **Standardul NIST-SP-800-30 Nr.53** |
| **Obiectiv** | Soluționarea eficientă și eficace a defecțiunilor hardware sau software;  Reducerea la minimum a efectelor dezastrelor naturale cauzate de un incendiu sau o inundație, prevenirea accesului neautorizat al persoanelor nefaste care pot deteriora serverele și dispozitivele de rețea. | | |
| **Evenimentele care cauzeaza riscul si rezultatele adverse ale impactului** |  | **Nivelul de impact** |  |
| **Low** | **Moderate** | **High** |
| High | Low Risk | Moderate Risk | Very High Risk |
| Moderate | Low Risk | Moderate Risk | High Risk |
| Low | Low Risk | Low Risk | Moderate Risk |
| **Valoarea probabilitatii** | **Low** | **Moderate** | **High** |

**Deosebiri**

|  |  |  |  |
| --- | --- | --- | --- |
| **Standard/**  **Criteriu** | **Standardul**  **ISO 27005** | **Metodologia Microsoft** | **Standardul NIST-SP-800-30 Nr.53** |
| **Tipuri de active** | 2 tipuri de active primare:  1. Procese (ori sub-procese) de business și activități  2. Informații | 3 tipuri de active:  1. Materiale  2. Nemateriale  3. IT | 2 tipuri de active:  1. Corporative  2. Necorporative |
| **Impact** | 2 tipuri de impact imediat:  1. Direct  2. Indirect | 1. Impact mare asupra afacerii (HBI)  2. Impact mediu asupra afacerii (MBI)  3. Impact mic asupra afacerii (LBI) | Amploarea impactului este: \*  1. scăzută (10),  2. medie (50)  3. ridicată (100). |
| **Probabilitate** | Se identifică utilizând tehnici de analiză cantitativă ori calitativă | 1. Mare. Probabilitea producerii unuia sau mai multor evenimente într-un an.  2. Medie. Efectele pot avea loc în doi sau trei ani.  3. Joasă. Apariția în timp de trei ani este puțin probabilă. | Indică probabilitatea ca o vulnerabilitate să poată fi exploatată de o sursă de amenințare, având în vedere controalele de securitate existente sau planificate.  1. Evaluare de probabilitate scăzută (0,1)  2. Medie (0,5)  3. Ridicată (1) |
| **Nivele de risc** | Evaluarea riscului are loc:  - Identificarea riscului  - Analiza riscului  - Evaluarea riscului | Evaluarea riscului:  - Planificare  - Colectarea coordonată a datelor  - Prioritizarea riscurilor | Evaluarea riscului acțiunile pe care managementul superior (proprietarii misiunii) trebuie să le întreprindă pentru fiecare nivel de risc. Output – Nivel de risc scăzut (1-10), mediu (>10-50) sau ridicat (>50) |
| **Calcularea riscului** | *Risc = probabilitatea de exploatare a unei vulnerabilități de amenințare x Impactul total al vulnerabilității exploatate* | *Risc = Ameninţare x Vulnerabilitate x Valoarea activului* | *Risc = determinarea probabilității x analiza impactului* |

\* Factorii datelor și sistemelor de luat în considerare ar trebui să includă importanța pentru misiunea organizației; sensibilitate și criticitate (valoare sau importanță); costurile asociate; pierderea confidențialității, integrității și disponibilității sistemelor și datelor.