MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susținere
Șef departament:
FIODOROV Ion dr., conf.univ.
_____
„___” _____ 2024

CADRUL UNIC FORMAL DE INTEGRARE A CONTROALELOR DE SECURITATE A INFORMAŢIEI

Proiect de master

Student: _____ **Căldare Doina, gr. SI-221M**

Conducător: _____ **Bolun Ion, dr. hab. prof. univ.**

Consultant: _____ **Bulai Rodica, lect. univ.**

Chișinău, 2024

REZUMAT

la teza de master **„Cadrul unic formal de integrare a controalelor de securitate a informaţiei”**
a masterandei din grupa SI-221M, programul de studii **„Securitatea informațională”,**
CĂLDARE Doina

Teza este destinată elaborării unui cadru unic al controalelor de securitate a informaţiei și cuprinde introducerea, trei capitole, concluzii, bibliografia din 15 titluri şi este perfectată pe 58 pagini de text de bază.

În lucrare se abordează importanța standardelor de securitate a informațiilor și rolul acestora în definirea și implementarea controalelor de securitate. La fel, se identifică și descriu criteriile utilizate pentru caracterizarea și evaluarea controalelor de securitate a informațiilor. Aceasta implică o privire atentă la standarde recunoscute, precum ISO 27001, NIST 800-53 și CIS. Prin evidențierea asemănărilor și diferențelor dintre aceste standarde, lucrarea își propune să ofere o imagine detaliată, facilitând astfel procesul de selecție și adaptare a controalelor într-un cadru unic.

Se accentuează necesitatea și beneficiile dezvoltării unui cadru unic pentru integrarea acestor controale, oferind organizațiilor posibilitatea de a gestiona securitatea informațiilor în mod eficient. În cadrul lucrării se discută aspecte esențiale legate de caracteristicile generale ale unui cadru unic. Ulterior este propus un cadru unic al controalelor de securitate a informaţiei. Totodată, se oferă informații detaliate despre procesul și pilonii de bază prin care se dezvoltă și se implementează aceste măsuri de securitate.

În concluzie, lucrarea oferă o perspectivă clară despre cum organizațiile pot integra cu succes măsurile de securitate a informațiilor într-un cadru unic și eficient, contribuind la consolidarea securității datelor și a informațiilor sensibile.

Cuvinte-cheie: standarde, controale, cadru de securitate a informațiilor.

ABSTRACT

to the master thesis "**The unique formal integration framework of information security controls**"
of the master's student in group SI-221M, study programme "**Information Security**",
CĂLDARE Doina

The thesis is intended to develop a single framework for information security controls and comprises an introduction, three chapters, conclusions, bibliography of 15 titles and is completed on 58 pages of basic text.

The paper addresses the importance of information security standards and their role in defining and implementing security controls. It also identifies and describes the criteria used to characterise and evaluate information security controls. This involves a close look at recognised standards such as ISO 27001, NIST 800-53 and CIS. By highlighting the similarities and differences between these standards, the paper aims to provide a detailed picture, thus facilitating the process of selecting and adapting controls within a single framework.

It emphasises the need and benefits of developing a single framework for integrating these controls, enabling organisations to manage information security effectively. The paper discusses key issues related to the general characteristics of a single framework. Subsequently, a single framework of information security controls is proposed. Detailed information is also provided on the process and basic pillars through which these security measures are developed and implemented.

In conclusion, the paper provides a clear insight into how organisations can successfully integrate information security measures into a single, effective framework, helping to strengthen the security of sensitive data and information.

Keywords: *standards, controls, information security framework.*

CUPRINS

INTRODUCERE

Securitatea informatilor protejează informația de o gamă largă de amenințări și este caracterizată ca fiind cea care asigură și menține confidențialitatea, integritatea și disponibilitatea. Securitatea informațiilor reprezintă un aspect esențial în societatea digitală actuală, iar organizațiile din întreaga lume se confruntă cu numeroase amenințări cibernetice, care pot avea consecințe devastatoare asupra datelor sensibile și a funcționării corecte a proceselor de afaceri. Pentru a gestiona aceste amenințări și a proteja informațiile esențiale, multe organizații adoptă standarde și regulamente de securitate a informațiilor. Adesea, respectarea acestora poate fi copleșitoare, organizațiile se confruntă cu o diversitate de norme și cerințe, astfel, pentru a face față acestor complexități, identificarea și integrarea controalelor comune prevăzute în aceste standarde devine esențială.

Integrarea controalelor prevăzute în standardele de securitate a informațiilor într-un cadru unic reprezintă un aspect esențial în gestionarea riscurilor și asigurarea securității datelor în era digitală actuală. Odată cu creșterea continuă al amenințărilor cibernetice și a vulnerabilităților în sistemele informatice, este foarte important de pus accent pe problema dată cu o viziune riguroasă și o metodologie bine definită. Această lucrare se încadrează în domeniul securității informațiilor, un domeniu în continuă expansiune și evoluție, iar într-o lume în care datele devin din ce în ce mai valoroase și în care riscurile cibernetice pot avea impact devastator asupra întreprinderilor, integrarea eficientă a controalelor de securitate devine o necesitate primordială.

Scopul principal al lucrării este explorarea și dezvoltarea unui cadru unic și formal pentru integrarea controalelor de securitate. Obiectivele acestei lucrări constau din identificarea principalelor standarde și reglementări relevante în domeniul securității informațiilor, analiza detaliată a controalelor de securitate din standardele selectate și dezvoltarea unui model formal pentru integrarea controalelor de securitate.

Primul capitol include analiza controalelor în standardele de securitate a informațiilor. Mai întâi de toate se explorează importanța standardelor de securitate a informațiilor și rolul lor în definirea și implementarea controalelor de securitate. După care urmează prezentarea detaliată a controalelor incluse în standardele de top selectate, cum ar fi: ISO 27001, NIST 800-53 și CIS. Exemplificarea necesității și beneficiilor de dezvoltare a unui cadru unic pentru integrarea controalelor, va permite organizațiilor să gestioneze securitatea informațiilor mai eficient.

În al doilea capitol sunt identificate și descrise criteriile utilizate pentru caracterizarea și evaluarea controalelor de securitate a informațiilor, examinarea caracteristicilor esențiale și analiza detaliată a controalelor din standarde pentru a identifica asemănările și diferențele, facilitând astfel selecția și adaptarea acestora într-un cadru unic.

Capitolul 3 abordează aspecte referitoare la caracteristicile generale ale noului cadru. Se explorează procesul de dezvoltare și implementare a controalelor, evidențiind pilonii de bază ai acestui

cadru. Aceasta include aspecte precum elaborarea politicilor de securitate, implementarea tehnică a controalelor, gestionarea incidentelor de securitate și evaluarea periodică a eficacității sistemului de securitate. În esență, acest capitol oferă o viziune mai amplă asupra modului în care organizațiile pot construi și integra un cadru solid pentru gestionarea securității informațiilor, asigurându-se că aceasta este o prioritate continuă și eficientă în cadrul organizației.

Lucrarea dată, tinde să exploreze necesitatea și avantajele identificării, suplinirii și integrării controalelor comune din diferite standarde de securitate a informațiilor într-un cadru unic. Această abordare nu numai că va reduce complexitatea procesului de gestionare a securității informațiilor în organizații, dar va contribui și la îmbunătățirea eficienței proceselor de securitate cibernetică.

BIBLIOGRAFIE:

1. L. Johnson, ”Cybersecurity framework”, Secur. Control. Eval. Testing, Assess. Handb., no. February 2014, pp. 537– 548, 2020.

2. Austrilian Signals Directorate, „Information Security Manual”. Austrilian Government. Published: 21 september 2023.

3. Hertteli, Leevi. Improving IT administration security by using security controls based on security frameworks Jyväskylä: JAMK University of Applied Sciences, May 2022, 60 pages.

4. Security and Privacy Controls for Information Systems and Organizations Special Publication (SP) 800-53 Rev 5, U.S. Department of Commerce, 2020, [citat 13.09.2023]. Disponibil: https://doi.org/10.6028/NIST.SP.800-53r5

5. Petrus M.J. Delport, Oliver D. Tverr. Principles Towards Determining the Operational Effectiveness of Information Security Controls. Noroff University College, Kristiansand, 4619, Norway 2023

6. INTERNATIONAL STANDARD. ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements..

7. NIKITIN, Danila. Achieving privacy and iso 27001 standard. South-Eastern Finland: University of Applied Sciences, 2023. [citat 20.09.2023]. Disponibil: https://www.theseus.fi/bitstream/handle/10024/801074/Nikitin_Danila.pdf?sequence=2

8. National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. [citat 02.10.2023]. Disponibil: https://doi.org/10.6028/NIST.CSWP.29.ipd

9. Frayssinet, M., Esenarro, D., Juárez, F. F., y Díaz, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10(2), 123-141. [citat 10.10.2023]. Disponibil: https://doi.org/10.17993/3ctic.2021.102.123-141

10. PCI DSS GUIDE. PSI DSS Requirement, Compliance Levels, [citat 15.10.2023]. Disponibil: https://pcidssguide.com/pci-dss-compliance-levels/

11. Center for Internet Security. The 18 CIS Critical Security Controls. [citat 26.09.2023]. Disponibil: https://www.cisecurity.org/controls/cis-controls-list

12. H. Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards - A Review and Comprehensive Overview, 2022. [citat 09.10.2023]. Disponibil: https://doi.org/10.3390/electronics11142181

13. NIST Cybersecurity Framework vs ISO 27001/27002 vs NIST 800-53 vs Secure Controls Framework. [citat 17.11.2023]. Disponibil: https://www.complianceforge.com/faq/nist800-53-vs-iso-27002-vs-nist-csf-vs-scf

14. CIS Controls v8 Mapping to NIST SP 800- 53 Rev 5, Center for Internet Security, 2021.

15. F. Ghaffari, A. Arabsorkhi, „A New Adaptive Cyber-Security Capability Maturity Model”, 9th International Symposium on Telecommunications, IEEE, 2018. [citat 02.12.2023]. Disponibil: doi**:** 10.1109/ISTEL.2018.8661018