Universitatea Tehnică a Moldovei

MODEL DE CONFORMITATE PRIVIND REGLAMENTARILE DE SECURITATE CIBERNETICA ÎN SECTORUL BANCAR

COMPLIANCE MODEL FOR CIBERSECURITY REGULATIONS IN THE BANKING SECTOR

Student: **gr. SI-231M,**
Șpac Antonio

Coordonator: **Beșliu Victor**
Profesor universitar

Chișinău, 2025

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

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____ 2025

MODEL DE CONFORMITATE PRIVIND REGLAMENTARILE DE SECURITATE CIBERNETICA ÎN SECTORUL BANCAR

Proiect de master

Student: _____ **Șpac Antonio, SI-231M**

Coordonator: _____ **Beşliu Victor, prof. univ., dr**

Consultant: _____ **Cojocaru Svetlana, asist. univ.**

Chişinău, 2025

REZUMAT

Lucrarea explorează tema conformității cu reglementările de securitate cibernetică în sectorul bancar, începând cu identificarea reglementărilor relevante, precum GDPR, PCI DSS NIST, ISO 27001 si DORA. Primul capitol detaliază cerințele specifice pe care aceste reglementări le impun instituțiilor financiare, punând accent pe importanța protecției datelor personale, a sistemelor critice și a confidențialității informațiilor clienților. Se discută despre scopul acestor reglementări și despre implicațiile nerespectării lor, inclusiv sancțiunile financiare, reputația afectată a instituțiilor și impactul asupra încrederii clienților.

În continuare, se analizează cerințele de conformitate și impactul acestora asupra securității cibernetice, evidențiind modul în care aceste reglementări contribuie la crearea unui mediu mai sigur pentru clienți și la prevenirea incidentelor de securitate. Se examinează cadrul legal care susține aceste cerințe, inclusiv reglementările naționale și internaționale, și se discută despre responsabilitățile specifice ale instituțiilor financiare în contextul securității cibernetice, inclusiv obligația de a raporta incidentele de securitate în termene limitate.

Un alt capitol este dedicat evaluării nivelului de conformitate al instituțiilor financiare prin studii de caz și exemple practice, ce ilustrează atât realizările, cât și provocările întâmpinate. Se analizează diverse strategii adoptate de instituții pentru a atinge conformitatea și se oferă exemple de bune practici, precum utilizarea tehnologiilor avansate de criptare, autentificare multifactorială și implementarea unui sistem de management al securității informațiilor (ISMS).

Lucrarea investighează apoi dificultățile întâmpinate de băncile comerciale în implementarea măsurilor de conformitate, inclusiv lipsa resurselor, rezistența la schimbare din partea angajaților și complexitatea tehnologică a sistemelor existente. Se subliniază necesitatea unei culturi organizaționale care să sprijine securitatea cibernetică, punând accent pe colaborarea interdepartamentală și pe angajamentul conducerii, precum și importanța educației și formării continue a personalului în domeniul securității cibernetice.

În final, se formulează recomandări pentru îmbunătățirea conformității și reducerea riscurilor asociate cu neconformitatea, propunând soluții concrete, cum ar fi implementarea de politici interne mai stricte, instruirea angajaților și adoptarea unor tehnologii avansate de securitate, precum inteligența artificială și analiza comportamentală. Se discută despre importanța evaluărilor periodice de risc și a auditurilor interne, care să asigure o monitorizare constantă a conformității. Aceste sugestii sunt menite să ajute instituțiile financiare să navigheze provocările actuale, să îmbunătățească postura lor de securitate cibernetică și să asigure o protecție adecvată pentru datele clienților într-un peisaj digital în continuă schimbare.

ABSTRACT

The paper explores the theme of compliance with cybersecurity regulations in the banking sector, starting with the identification of relevant regulations such as GDPR, PCI DSS,DORA, ISO 27001 and NIST. The first chapter details the specific requirements imposed by these regulations on financial institutions, emphasizing the importance of protecting personal data, critical systems, and the confidentiality of client information. It discusses the purpose of these regulations and the implications of non-compliance, including financial penalties, the affected reputation of institutions, and the impact on customer trust.

Next, the paper analyzes the compliance requirements and their impact on cybersecurity, highlighting how these regulations contribute to creating a safer environment for customers and preventing security incidents. It examines the legal framework supporting these requirements, including national and international regulations, and discusses the specific responsibilities of financial institutions in the context of cybersecurity, including the obligation to report security incidents within set deadlines.

Another chapter is dedicated to evaluating the level of compliance of financial institutions through case studies and practical examples that illustrate both achievements and challenges encountered. It analyzes various strategies adopted by institutions to achieve compliance and provides examples of best practices, such as the use of advanced encryption technologies, multi-factor authentication, and the implementation of an Information Security Management System (ISMS).

The paper then investigates the difficulties faced by commercial banks in implementing compliance measures, including resource shortages, employee resistance to change, and the technological complexity of existing systems. It emphasizes the necessity of an organizational culture that supports cybersecurity, highlighting the importance of interdepartmental collaboration and leadership commitment, as well as the importance of continuous education and training of staff in the field of cybersecurity.

Finally, recommendations are formulated to improve compliance and reduce the risks associated with non-compliance, proposing concrete solutions such as implementing stricter internal policies, training employees, and adopting advanced security technologies, including artificial intelligence and behavioral analysis. The importance of periodic risk assessments and internal audits is discussed to ensure continuous monitoring of compliance.

CUPRINS

INTRODUCERE

În era digitalizării accelerate, sectorul bancar se confruntă cu provocări fără precedent în ceea ce privește securitatea cibernetică. Transformările tehnologice, cum ar fi adoptarea soluțiilor de banking online, a serviciilor de plăți digitale și a aplicațiilor mobile, au îmbunătățit accesibilitatea și eficiența serviciilor financiare. Totuși, aceste progrese au venit cu un cost semnificativ: expunerea sporită la amenințări cibernetice. Instituțiile financiare devin ținte atractive pentru atacatori, iar riscurile asociate cu violările de securitate și pierderea datelor personale sunt în continuă creștere. În acest context, conformitatea cu reglementările de securitate cibernetică devine o prioritate crucială pentru asigurarea integrității și confidențialității datelor clienților.

Reglementările precum Regulamentul General privind Protecția Datelor (GDPR), Standardul de Securitate pentru Datele Industriei de Plăți (PCI DSS) și cadrul de standarde NIST (National Institute of Standards and Technology) oferă un cadru esențial pentru gestionarea riscurilor cibernetice. Printre principalele cerințe impuse de aceste reglementări se numără:

- protecția datelor personale: GDPR impune băncilor să adopte măsuri stricte de protecție a datelor personale, asigurând astfel transparența și controlul utilizatorilor asupra informațiilor lor;
- securitatea tranzacțiilor: PCI DSS se concentrează pe protejarea datelor de plată, asigurându-se că toate organizațiile care procesează carduri de credit respectă standarde riguroase de securitate;
- managementul riscurilor: NIST oferă un set de bune practici și orientări pentru gestionarea securității informațiilor, promovând un cadru adaptabil la nevoile specifice ale fiecărei organizații.

Organismele de reglementare, precum Banca Națională a României (BNR) și Autoritatea Bancară Europeană (EBA), joacă un rol esențial în promovarea conformității cu aceste reglementări, monitorizând și evaluând implementarea măsurilor de securitate de către instituțiile financiare. Aceste instituții nu doar că impun standarde de securitate, ci și oferă suport și îndrumare în adaptarea la un peisaj digital în continuă schimbare.

Această cercetare își propune să analizeze implementarea reglementărilor de securitate cibernetică în sectorul bancar, evaluând eficiența măsurilor adoptate de bănci în protejarea datelor și prevenirea riscurilor. Printr-o analiză detaliată a conformității cu standardele internaționale, acest studiu va oferi perspective valoroase asupra modului în care instituțiile financiare pot naviga provocările complexe ale securității cibernetice și pot contribui la crearea unui mediu financiar mai sigur și mai fiabil pentru clienți. În final, se va sublinia importanța unei abordări proactive și integrate în gestionarea securității cibernetice, care să răspundă atât cerințelor legale, cât și nevoilor clienților.

BIBLIOGRAFIE

[1] „A Brief Look at 4 Major Data Compliance Standards: GDPR, HIPAA, PCI DSS, CCPA”, Penta Security Inc. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.pentasecurity.com/blog/4-data-compliance-standards-gdpr-hipaa-pci-dss-ccpa/

[2] O. Nir, „The Complete List of Data Security Standards”, Reflectiz. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.reflectiz.com/blog/data-security-standards/

[3] „Cybersecurity Framework”, *NIST*, nov. 2013, Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.nist.gov/cyberframework

[4] D. Kosutic, „What is ISO 27001? An easy-to-understand explanation.” Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://advisera.com/27001academy/what-is-iso-27001/

[5] „Digital Operational Resilience Act (DORA)”. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora?utm_source=chatgpt.com

[6] „Document Library”, PCI Security Standards Council. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.pcisecuritystandards.org/document_library/

[7] „General Data Protection Regulation (GDPR) – Legal Text”, General Data Protection Regulation (GDPR). Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://gdpr-info.eu/

[8] „Basel III: international regulatory framework for banks”, dec. 2017, Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.bis.org/bcbs/basel3.htm

[9] „Cybersecurity Framework”, *NIST*, nov. 2013, Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.nist.gov/cyberframework

[10] „Guidelines on ICT and security risk management | European Banking Authority”. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.eba.europa.eu/guidelines-ict-and-security-risk-management

[11] „Tokenization vs. Encryption for Data”, Skyhigh Security. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.skyhighsecurity.com/cybersecurity-defined/tokenization-vs-encryption.html

[12] „OnDemand Webinar I Defense in Depth – Filling the Gaps to Detect and Stop Lateral Movement”. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.bankinfosecurity.com/importance-mfa-in-banking-a-17891

[13] „Studiu Deloitte: organizațiile din domeniul serviciilor financiare încep să înregistreze progrese în implementarea noului regulament UE privind reziliența operațională digitală, DORA”, Deloitte Romania. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www2.deloitte.com/ro/ro/pages/about-deloitte/articles/studiu-deloitte-organizatiile-din-domeniul-serviciilor-financiare-incep-sa-inregistreze-progrese-in-implementarea-noului-regulament-ue-privind-rezilienta-operationala-digitala-dora.html

[14] agerpres.ro, „Securitatea cibernetică rămâne un risc major pentru băncile europene (studiu)”. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://agerpres.ro/economic/2024/02/12/securitatea-cibernetica-ramane-un-risc-major-pentru-bancile-europene-studiu--1247192?utm_source=chatgpt.com
[15] „Reglementare și supraveghere bancară | Banca Națională a Moldovei”. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.bnm.md/ro/content/reglementare-si-supraveghere-bancara
[16] „Victoriabank aplică practicile europene privind protecția datelor personale - MoldStreet”. Data accesării: 13 ianuarie 2025. [Online]. Disponibil la: https://www.mold-street.com/?go=news&n=12473&utm_source=chatgpt.com
[17] M. ENACHI și L. BUZILĂ, „AUDITUL INTERN ÎN SISTEMUL CONTROLULUI FINANCIAR DE STAT”, sep. 2023, doi: 10.5281/ZENODO.8363358.