TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Jan Erik Kriisk 212063IVCM

NIST CSF 2.0 Implementation Challenges in the Banking Sector

Master's thesis

Supervisor: Sille Arikas

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Jan Erik Kriisk 212063IVCM

NIST CSF 2.0 rakendamise väljakutsed pangandussektoris

Magistritöö

Juhendaja: Sille Arikas

Tallinn 2025

Abstract

Cybersecurity is a critical concern for financial institutions, as they manage vast amounts of sensitive data and operate within a highly regulated environment. Banks increasingly rely on structured frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to strengthen cybersecurity resilience. The 2024 release of NIST CSF 2.0 significantly broadens the framework's scope and highlights the need to assess its relevance and implementation challenges within the banking sector. However, existing research has widely overlooked the unique implementation challenges financial institutions face under the new framework. This study addresses this gap by examining banks' primary obstacles when adopting NIST CSF 2.0 and identifying strategies to enhance its effective implementation.

The research employs a qualitative approach, leveraging a case study of a Baltic-wide bank that conducted a self-assessment against NIST CSF 2.0. This assessment, structured around maturity ratings, justification statements, and gap remediation actions, is the primary data source for identifying implementation challenges. Additionally, expert interviews with information security professionals from other financial institutions from the Baltic region provide complementary insights into sector-specific difficulties and best practices. Thematic analysis is applied to both data sources, categorizing implementation challenges into structured themes to reveal common patterns and sector-specific barriers.

The findings highlight several recurring challenges, including difficulties enforcing cybersecurity controls, aligning the framework with regulatory requirements, and ensuring effective security monitoring. Banks also struggle to integrate NIST CSF 2.0 into existing cybersecurity frameworks, manage third-party risks, and address governance gaps. Resource constraints—often cited as a significant challenge in broader cybersecurity literature, have not been as prominent in this case study, suggesting that large financial institutions may have sufficient cybersecurity funding but still face operational and technical hurdles. Interviews further highlighted the challenge of including cybersecurity maturity assessments in executive-level reporting to secure strategic support for implementation efforts.

This research provides practical recommendations for financial institutions adopting NIST CSF 2.0. Key strategies include establishing clear governance structures, strengthening security automation and monitoring, developing cross-mapping frameworks for regulatory alignment, and embedding cybersecurity awareness into corporate culture. The study contributes to understanding cybersecurity framework adoption in the banking sector, offering insights that can inform both academic discourse and industry practices on NIST CSF 2.0 implementation.

The thesis is written in English and is 43 pages long, including 8 chapters and 1 figure and 1 table.

Annotatsioon

Küberturvalisus on finantsasutuste jaoks kriitilise tähtsusega, kuna nad haldavad suures mahus tundlikke andmeid ja tegutsevad rangelt reguleeritud keskkonnas. Küberturvalisuse vastupanuvõime tugevdamiseks tuginevad pangad üha enam struktureeritud raamistikutele, näiteks National Institute of Standards and Technology küberturvalisuse raamistik (NIST CSF). 2024. aastal uuendatud raamistik NIST CSF 2.0 vajab omakorda selle kohaldatavuse ja rakendamise väljakutsete hindamist pangandussektoris. Olemasolevad uuringud on suuresti jätnud tähelepanuta finantsasutuste unikaalsed väljakutsed raamistiku uue versiooni rakendamisel. Käesolev lõputöö, uurib peamisi takistusi, millega pangad NIST CSF 2.0 kasutuselevõtul silmitsi seisavad ja pakub strateegiaid selle tõhusamaks rakendamiseks.

Lõputöös kasutatakse juhtumiuuringule tuginedes kvalitatiivset lähenemist, mis analüüsib Baltikumi ülese panga NIST CSF 2.0 järgset enesehindamist. Enesehindamine põhines küpsusastmete hinnangutel, põhjendustel ja puudujääkide kõrvaldamise tegevuskavadel ning peamine andmeallikas rakendamise takistuste tuvastamiseks. Lisaks annavad infoturbe spetsialistide intervjuud erinevatest finantsasutustest täiendavaid teadmisi sektori-spetsiifilistest raskustest ja parimatest tavadest. Andmete analüüsimiseks rakendatakse temaatilist analüüsi, kategoriseerides rakendamise väljakutsed struktureeritud teemadesse, et tuua esile ühised mustrid ja sektori-spetsiifilised takistused.

Tulemused toovad esile mitmeid korduvaid väljakutseid, sealhulgas raskused küberturvalisuse kontrollide jõustamisel, raamistiku vastavusse viimine regulatiivsete nõuetega ja tõhusa turvamonitooringu tagamine. Pangad seisavad silmitsi ka NIST CSF 2.0 integreerimisega olemasolevatesse küberturvalisuse raamistikesse, kolmandate osapoolte riskijuhtimisega ning juhtimise ja vastutuse puudujääkidega. Märkimisväärselt ei olnud ressursipiirangud – mida küberturvalisuse üldises kirjanduses sageli peetakse suureks takistuseks – selles juhtumiuuringus esmale esinevad, mis viitab sellele, et suured finantsasutused võivad omada piisavat küberturvalisuse rahastust, kuid seisavad silmitsi pigem operatiivsete ja tehniliste takistustega. Intervjuud rõhutasid ka raskusi

küberturvalisuse küpsushinnangute tõlkimisel juhtimistasandi aruandluseks, et tagada strateegiline toetus rakendamisalgatustele.

Lõputöö pakub praktilisi soovitusi finantsasutustele NIST CSF 2.0 kasutuselevõtuks. Peamised strateegiad hõlmavad selgete juhtimisstruktuuride loomist, turvaautomaatika ja -monitooringu tugevdamist, regulatiivse vastavuse tagamiseks ristkaardistamise raamistikkude arendamist ning küberturvalisuse teadlikkuse juurutamist ettevõttekultuuri. Käesolev uurimus annab olulise panuse pangandussektori küberturvalisuse raamistikuga seotud väljakutsete mõistmisse, pakkudes teadmisi, mis võivad aidata kaasa nii akadeemilisele diskursusele kui ka tööstuspraktikatele NIST CSF 2.0 rakendamise osas.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 43 leheküljel, 8 peatükki, 1 joonist ja 1 tabelit.