Development and implementation of security standards and policies for organizations

By

Maratov Daniyar
Zhurekbay Abay
Dauitkanov Zhiger

Department of Cybersecurity
Astana IT University

6B06301 — Educational Program
Supervisor: Gulsim Tulepova

June 2025
Astana

Author's dedication

We, the authors of this thesis, wholeheartedly dedicate this work to Astana IT University, an institution that has not only provided us with quality education but also instilled in us a sense of responsibility and purpose as future professionals in the field of cybersecurity. The academic environment fostered by the university challenged us to think critically, act ethically, and contribute meaningfully to the evolving landscape of information security. We are especially grateful for the university's emphasis on combining theoretical understanding with practical application, which was instrumental in shaping the dual focus of this research.

Our deepest appreciation goes to our thesis supervisor, Ms. Gulsim Tulepova, whose expert guidance, insightful feedback, and unwavering support were pivotal throughout every phase of this work. Her dedication to academic excellence, her high standards, and her constant encouragement motivated us to reach beyond the minimum and strive for quality and relevance in our research.

This thesis stands as a testament to the knowledge and mentorship we received during our time at the Department of Cybersecurity. It is our sincere hope that this work will contribute to the academic discourse at Astana IT University and serve as a resource for future students and researchers exploring security standards and policy development.

Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and that it has not been submitted for any other academic award. Except where indicated by specific references in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: ..... DATE: .....

Abstract

This diploma thesis explores the development and implementation of information security standards and policies within organizations, focusing on integrating international best practices with Kazakhstan's regulatory context. The study compares major cybersecurity frameworks – ISO/IEC 27001:2022, the NIST Cybersecurity Framework (CSF) 2.0, and the EU GDPR – and analyzes their relevance and adaptability to Kazakhstan, considering national laws like the Law on Informatization and Law on Personal Data. It also details the methodology and results of developing a web-based and mobile solution to help a fictional company ("QazFinTech Bank") adopt and operationalize security standards and policies. The Literature Review provides a comparative analysis of the frameworks and local regulations. The Methodology outlines how theoretical research and practical development were conducted. The Practical Implementation chapter describes the design of a website (HTML/CSS/JS) and a mobile application (React Native with a Node.js backend) that assist organizations in policy adoption and compliance. In Development of Security Standards and Policies, original policy documents and control standards tailored to Kazakhstani organizations are created, bridging ISO/NIST controls with local legal requirements; this includes tables mapping controls to policies, and defining user roles with access levels. The Results and Discussion demonstrate how these standards and tools would function in the QazFinTech Bank scenario, analyzing benefits, limitations, and regulatory impacts. Finally, the Conclusion summarizes findings, highlights the potential for broader adoption at a national level, and suggests avenues for future research. This work aims to contribute both a practical toolkit and strategic guidance for organizations in Kazakhstan seeking to enhance their cybersecurity posture in line with international standards and local laws.

List of Tables

Table **Page**

List of Figures

Figure **Page**

Table of Contents

1 Introduction

In today's digital era, organizations face escalating cybersecurity threats and increasingly stringent regulatory requirements for protecting information. Businesses and governments worldwide have turned to established security standards and frameworks to manage cyber risks systematically. In Kazakhstan, like in many countries, there is a growing need to harmonize global best practices with local laws to safeguard data and ensure compliance. Astana IT University's interest in this topic reflects the national priority on strengthening information security, as critical sectors (e.g. finance, government services) digitalize and integrate with global networks. This thesis titled "Development and Implementation of Security Standards and Policies for Organizations" examines how organizations can effectively implement information security standards and policies. It addresses both the theoretical frameworks and the practical tools needed to enforce those standards. The research is motivated by challenges observed in aligning international cybersecurity standards – such as ISO/IEC 27001, NIST CSF, and GDPR – with Kazakhstan's legal and operational context. Although frameworks like ISO 27001 are internationally recognized for improving an organization's security management, their adoption must consider national legislation (for example, Kazakhstan's Law "On Informatization" and the Law "On Personal Data and Its Protection"). Organizations in Kazakhstan, especially in regulated industries like banking, must navigate requirements from the National Bank and other authorities while also aspiring to global best practices. Research Objectives: The primary objectives of this thesis are: (1) to perform a comparative analysis of key international cybersecurity standards (ISO/IEC 27001:2022, NIST CSF 2.0, and GDPR) and determine how they can be adapted to Kazakhstan's context; (2) to develop a conceptual framework and prototype tools (web and mobile applications) that assist organizations in implementing these standards and crafting compliant security policies; (3) to create a set of original security policies and controls for a model Kazakhstani organization, integrating international standards with local regulatory compliance; and (4) to evaluate the implementation through a fictional use-case (QazFinTech Bank) and discuss the outcomes, benefits, and challenges. Significance: By addressing these objectives, the thesis aims to provide both scholarly insight and practical solutions. From an academic perspective, it contributes to understanding the interplay between global cybersecurity frameworks and domestic regulations. From a practical standpoint, it delivers a prototype "toolkit" – a website and mobile app –

that could be further developed to help real organizations in Kazakhstan manage their information security programs. The fictional case study of QazFinTech Bank is used as a realistic scenario to ground the discussion in practical application. Ultimately, this research supports Kazakhstani organizations in bolstering their cybersecurity maturity in an era of international data exchange and sophisticated cyber threats. The remainder of this thesis is structured as follows: the Problem Statement defines the core problems and gaps this research addresses. The Literature Review surveys relevant standards and laws, comparing their content and implications. The Methodology chapter explains the research approach, including how the security framework integration and software development were carried out. The Practical Implementation chapter describes the developed web and mobile solutions and how they function in the case study scenario. The Development of Security Standards and Policies chapter presents the custom-designed policies, standards, and control mappings for the fictional organization. The Results and Discussion chapter evaluates how the proposed standards and tools would operate in practice, examining benefits, limitations, and compliance outcomes. Finally, the Conclusion and Future Work chapter summarizes key findings, recommends how these efforts could be scaled nationally, and suggests directions for future research.

2 Problem Statement

Organizations in Kazakhstan face a dual challenge in information security management: they must adhere to international best practices to effectively mitigate cyber risks, while also complying with local regulatory requirements. This dual mandate can be problematic due to gaps between global frameworks and local laws, and a lack of readily available guidance on integrating the two. Key problems addressed in this thesis include:

- **Lack of Integrated Security Frameworks.** Many Kazakhstani organizations do not have a comprehensive information security management system (ISMS) in place. For instance, the National Bank of Kazakhstan noted the need for banks to establish information security management systems and formal security procedures. However, there is uncertainty about which framework to adopt (e.g., ISO vs. NIST) and how to align it with Kazakhstan's context. This results in inconsistent security postures and difficulties in demonstrating compliance.

- **Alignment with International Standards.** Frameworks like ISO/IEC 27001 and NIST CSF offer structured approaches to security. Yet, adoption of these standards in Kazakhstan has been limited, partly due to a lack of localized guidance. The question arises: how can ISO 27001:2022 and NIST CSF 2.0 be adapted to the legal, cultural, and operational environment of Kazakhstani organizations?

- **Compliance with Data Protection Regulations.** Kazakhstan's Law "On Personal Data and Its Protection" (2013) imposes requirements on data handling. Organizations need to align internal policies with GDPR-like principles (consent, minimization, breach notification), while also respecting local mandates such as data localization.

- **Operational Gap – Lack of Tools for Implementation.** Even when policies exist, many organizations lack systems to enforce them. Employees may not be aware, controls may be inconsistently applied, and audits reveal gaps. A centralized tool for policy enforcement, incident response, training, and compliance tracking is lacking.

Fictional Case Focus – QazFinTech Bank. This thesis uses a fictional mid-size Kazakhstani financial organization to examine how ISO 27001, NIST CSF, and GDPR principles can be integrated into a unified security policy framework adapted to national law. It explores what a practical implementation tool for this integration might look like.

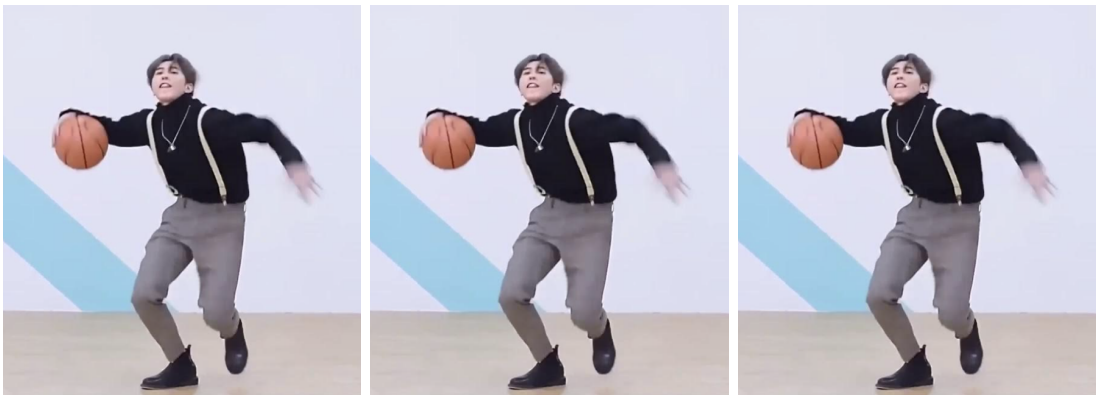
Summary. The core problem is bridging the gap between international cybersecurity frameworks and local organizational practice in Kazakhstan. This includes aligning standards with laws, developing policy, and applying them through enforceable tools to

enhance resilience and compliance.

3 Chapter Title

$$Q = \frac{1}{h^{3N} N!} \int \int e^{-\beta H(p,q)} dpdq \tag{3.1}$$

$$H(p,q) = \sum_{i=1}^{N} \frac{p_i^2}{2m_i} + V(q) \tag{3.2}$$



(a) (b) (c)

Figure 3.1: Description of this figure

3.1 Section title

AITU AITU

3.2 Section title

AITU AITU

3.2.1 Subsection title

AITU AITU

4 Conclusion

AITU

Term AA	Term BB	Term CC	Term DD
0.893	-0.308	-0.0498	-0.0498
0.248	-0.099	-0.0414	-0.0488

Table 4.1: Describe your table

A Appendix A

Begins an appendix

Bibliography