Universal Library of Business and Economics Original Article

ISSN: 3064-9951 | Volume 1, Issue 2

Open Access | PP: 57-59

DOI: https://doi.org/10.70315/uloap.ulbec.2024.0102010

Nataliia Stashevska on Non-Functional Requirements in Cybersecurity: How to Anticipate and Minimize Risks in Developing Government and Financial Platforms

Nataliia Stashevska

Expert in Business Analysis and Digital Transformation.

Abstract

The article discusses the methodology for integrating cybersecurity into the software development lifecycle through the lens of non-functional requirements (NFRs). The purpose of the study is to demonstrate that proactively identifying and managing NFRs is a fundamental approach to minimizing risks when creating critical platforms in the government and financial sectors. Based on the analysis of practical cases, such as MassMutual, State Street and SoftServe, the paper systematizes methods for translating regulatory norms (NYDFS, HIPAA) and industry standards (SOC, ITIL) into specific, measurable and testable non-functional requirements. The article proves that a business analyst with cybersecurity competencies ensures that the developed systems comply with security requirements by default (Security by Design), which reduces the cost of eliminating vulnerabilities and increases the overall resilience of digital assets.

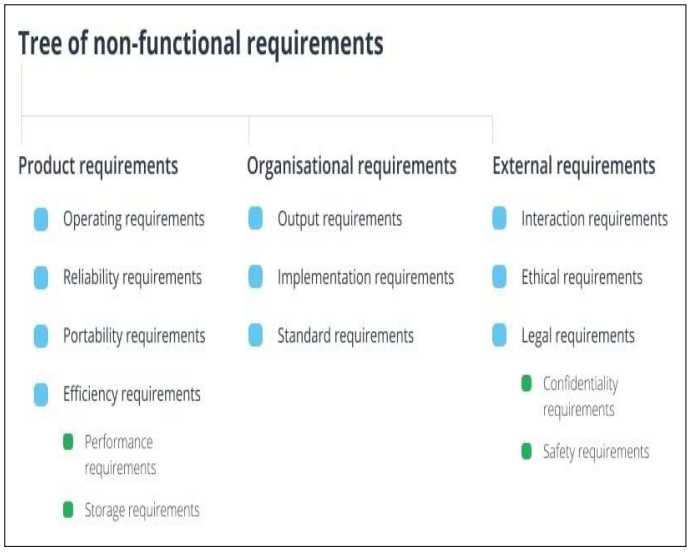
Keywords: *Non-Functional Requirements, Cybersecurity, Business Analysis, Risk Management, Fintech, Government Platforms, Security by Design, Compliance.*

Digital transformation in government and financial institutions comes with an exponential increase in cyber threats. A successful attack on such platforms can lead not only to direct financial losses but also to systemic failures and a loss of citizen trust. The traditional development approach, where security is treated as a separate testing phase prior to deployment, has proven inadequate. Vulnerabilities embedded in the system architecture at early stages require significantly higher costs to fix than preventing them proactively.

The relevance of this research lies in the need to shift the paradigm toward "Security by Design". This approach implies that security requirements must be an integral part of project specifications from the very beginning. The aim of this article is to outline a methodology for applying non-functional requirements (NFRs) as a primary tool to anticipate and mitigate risks. Using practical case studies, it demonstrates how business analysis ensures the integration of cybersecurity requirements into the core of developing systems.

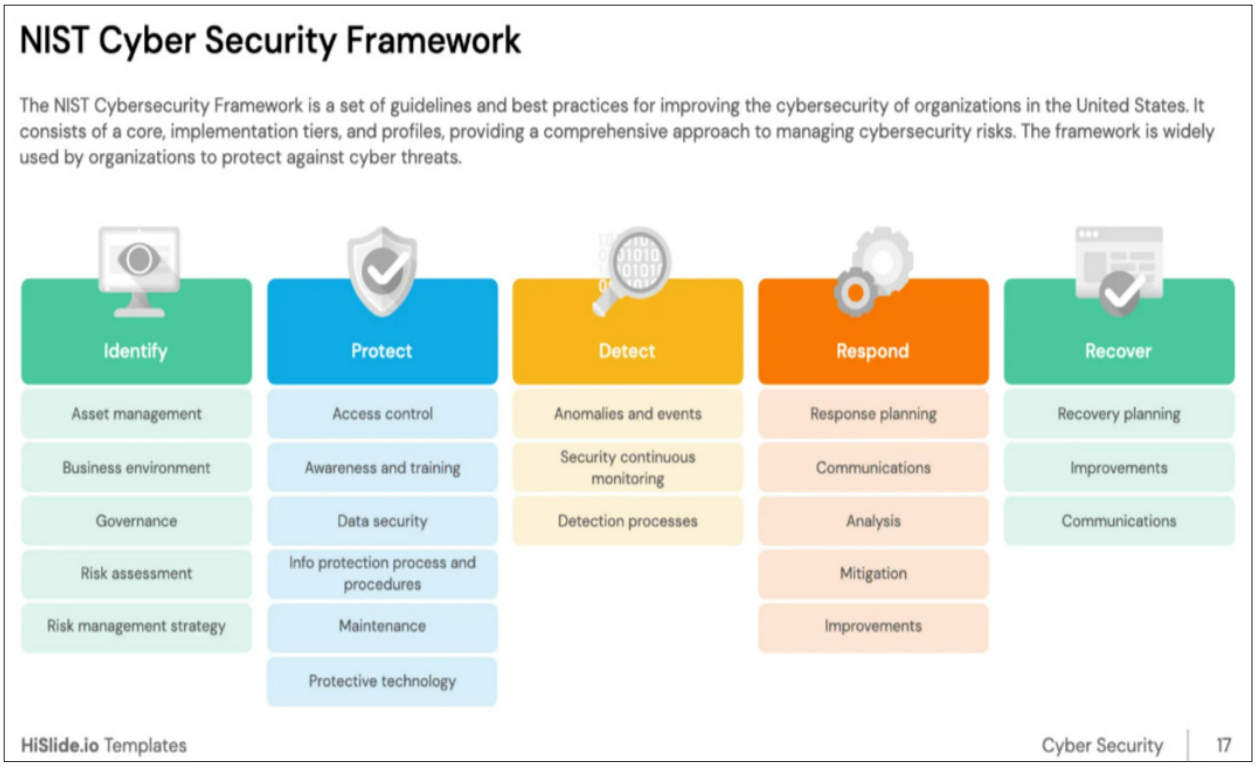
In software engineering, requirements are generally divided into functional requirements, which describe what a system should do, and non-functional requirements (NFRs), which define how the system should perform these functions. NFRs include attributes such as performance, scalability, reliability, and, crucially, security [1]. It is within the NFR category that aspects related to confidentiality, integrity, and availability of data are formalized.

Despite their importance, NFRs are often overlooked in the early stages of a project because they are less obvious to business stakeholders and more difficult to formalize. This leads to systems that function as intended but remain vulnerable to attacks. Modern cybersecurity frameworks, such as the NIST Cybersecurity Framework, provide a structure for risk management but do not dictate specific system-level requirements [2]. The task of the business analyst is to translate the high-level goals of these frameworks and regulatory standards into clear and verifiable NFRs.



- The process of identifying and analyzing non-functional requirements (NFRs) in cybersecurity is a systematic task of the business analyst and involves several stages.

- Regulatory environment analysis. In the MassMutual project, work included drafting internal policies in compliance with NYDFS requirements and gathering requirements for a cyber platform intended for governmental certifications. This is a direct example of translating legal norms into specifications for developers.
- Mapping to industry standards. At State Street, efforts were undertaken to map business processes to SOC security controls. This ensures that operational activities comply with widely accepted audit and security standards.
- Defining quality attributes. Work at SoftServe to optimize cybersecurity processes according to ITIL resulted in a 15% reduction in risks. This was achieved through formalizing requirements for incident management, change management, and access control processes.
- The effectiveness of the NFR-based approach is most evident in high-stakes projects:
- Financial sector (MassMutual, State Street). Developing requirements for financial platforms demands consideration of NFRs such as data encryption in transit and at rest, granular access control, audit logging, and fault tolerance. Clearly defined requirements based on NYDFS standards and SOC controls simplify audits and demonstrate due diligence to regulators.
- Government sector (Ukrainian State Court Administration). When creating an electronic document management system for courts in Ukraine, potential security risks were identified and minimized. NFRs in this context addressed the integrity of legally significant documents, access control to case materials, and system availability for authorized users.
- Business continuity (SoftServe). The project for emergency migration of servers and client data from Europe and the U.S. during wartime served as an extreme test of NFRs such as availability and data integrity. Successful execution was made possible by pre-established protocols and architectural solutions incorporated into the system at the design stage.



The analysis demonstrates that systematic work with non-functional requirements (NFRs) is not an optional addition but a mandatory condition for creating secure and resilient digital platforms in the public and financial sectors. A business analyst with competencies in cybersecurity plays a central role in integrating security requirements into the DNA of the product.

Practical cases show that this approach not only ensures compliance with complex regulatory requirements but also effectively manages risks, maintains business continuity in critical situations, and reduces the total cost of system ownership by minimizing costly rework at later stages. For organizations striving for digital leadership, investing in developing competencies in NFR analysis should become a strategic priority.

REFERENCES

1. Glinz, M. On Non-Functional Requirements // Proceedings of the 15th IEEE International Requirements Engineering Conference. 2007. P. 21–26.

2. Chung, L., Nixon, B. A., Yu, E., & Mylopoulos, J. Non-Functional Requirements in Software Engineering. // Kluwer Academic Publishers. 2000.

3. OWASP Top Ten Web Application Security Risks. // Open Web Application Security Project. 2021. URL: https://owasp.org/www-project-top-ten/.

4. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. // National Institute of Standards and Technology (NIST). 2018.

Citation: Nataliia Stashevska, "Nataliia Stashevska on Non-Functional Requirements in Cybersecurity: How to Anticipate and Minimize Risks in Developing Government and Financial Platforms", Universal Library of Business and Economics, 2024; 1(2): 57-59. DOI: https://doi.org/10.70315/uloap.ulbec.2024.0102010.