university of groningen

faculty of science and engineering

Final Project Plan

Automating the NIS2 Framework Compliance Evaluation

Tudor Dragan (s4394887)

Contents

1 Introduction

1.1 Thesis Outline

Critical Infrastructure is defined by the European Union (EU) as the systems and services required for maintaining the ”vital functioning of society” [1]. This term encompasses national power grids, water supply, transportation and telecommunication networks etc. These systems have become the target of various attacks, coming from actors looking to destabilize or create chaos in a country or region. These attacks are often against the digital systems controlling critical infrastructure. Thus, protecting critical infrastructure is paramount to ensuring the normal functioning of society. The EU recognizes the threat to this infrastructure and has created a directive aimed at ensuring a high common level of cybersecurity across all member states. The first such directive was the Network and Information Systems Directive (NIS).

Recently, a new directive for cybersecurity under the name of NIS2 [2] has been developed as the successor of NIS. This new directive enforces stricter measures and expands the criteria that determine which companies need to comply with the new regulation. According to the Dutch governmental timeline, the NIS2 directive will be implemented as the Cybersecurity Act in the ”third quarter of 2025” [3].

1.2 Project Definition

1.2.1 Problem definition

With new developments in regulations come new mandatory requirements for companies to establish a stronger overall cybersecurity stance, as well as increased accountability for executives, when it comes to the cyber-readiness of their firms. Thus, many companies struggle to understand the following:

- Whether or not they fall under the regulation of NIS2?
- What measures are required by law to comply with NIS2?
- How should these measures be implemented?

As a provider of managed cybersecurity services, Northwave’s mission is to help its customers navigate these regulatory requirements and help with the implementation of appropriate measures. Primarily, they have created a framework for the assessment and reporting of NIS2 compliance. However, these reports take a large amount of time and resources to be created. Interviews have to be done first and then a comprehensive report covering all of the compliance criteria has to be created. Thus, they are interested in automating (parts of) this assessment and are looking for the most effective way to do so. Thus, my project will be aimed at developing a methodology to automate these assessments.

1.2.2 Motivation

Northwave is looking to make use of cutting-edge technologies to streamline its processes and has placed a large amount of its research efforts into discovering how the use of Large Language Models (LLMs) can benefit the company. In applications that require the processing of large amounts of unstructured textual data, such as interview transcripts, LLMs can greatly reduce the time needed to create a comprehensive and well-structured report. This is especially applicable to the use case that I am investigating, automating the reports regarding compliance with cyber security frameworks.

By virtue of the extended reach of NIS2, many companies now need assistance with navigating these new regulations. This is an important business case for Northwave and introducing automation into the reporting process would free up resources at the company, to focus on helping out more clients.

1.2.3 Goals and research questions

The primary goal of the project is to help the consultant team that provides the NIS2 compliance assessment service automate the reporting process. A secondary goal is to analyze how this assessment service can lead to new potential customers for Northwave.

Central research question: How can Northwave effectively support companies in achieving and maintaining compliance with the NIS2 directive through the development of a scalable and automated assessment framework?

This question can be broken down into the following subquestions:

- What is the state of the art in cybersecurity frameworks?
- What is the most adequate methodology for conducting the compliance assessment for NIS2?
- How can the assessment be automated?

1.2.4 Boundary conditions

The project is scheduled to last between 06/01/2025 and 30/06/2025. The project will involve literature research to establish the state of the art in cyber security framework assessment and automation. Policy aspects will include understanding the different frameworks and how compliance is assessed. Business aspects are also part of the project, with interviews and assessments being conducted as a way to introduce potential customers to Northwave and present areas where help might be needed. The science/policy/business distribution is likely to be 40/20/40.

1.2.5 Intended results

The primary deliverable of this project is a report containing all of the above-outlined components. A comprehensive literature review of cybersecurity frameworks and their assessment methodology, from both the scientific and policy perspectives. This will result in concrete recommendations for Northwave on how to conduct and automate its interview process. A second result will be related to the business perspective and will recommend Northwave strategies on how to use NIS2 compliance interviews to acquire new customers. The second deliverable will be a ~~demo~~ implementation of the automation methodology. The aim of this is to showcase the potential for LLMs in reducing the time it takes to aggregate information and create reports, allowing Northwave to reach out to and help more companies

1.2.6 Scope

The project will focus specifically on Northwave and its customers. The internal department that the project is for is the business consultancy department. The main focus will be on determining their customers' compliance with NIS2. However, the automation methodology should be easily applicable to other assessments. Provided time allows the project could be extended to include other frameworks.

1.2.7 Impact

This project has the potential to significantly impact the cybersecurity stance of organizations by providing efficient means to assess and achieve compliance with the NIS2 directive. By developing an automated compliance assessment framework, the project will help reduce the time and resources required for organizations to meet regulatory requirements. Thus, there will be a wider adoption of robust cybersecurity practices, ultimately leading to a more resilient infrastructure at the level of the EU. The project will have a secondary impact on the ability of Northwave to perform assessments faster, and possibly obtain more customers.

1.3 Work Breakdown Structure

Subproject	Title	Time Requirement
1	Cyber Security Framework Requirements	3
2	Northwave Assessment Process Understanding	4
3	Reporting Automation Methodology + Automating the Reporting	5+5

Subproject 1: In this subproject, I will conduct a comprehensive review of existing cybersecurity frameworks and standards to understand their strengths and limitations. This will involve analyzing widely adopted frameworks such as ISO 27001 [4], CIS Controls, and NIST CSF [5] to identify elements that can inform the NIS2 compliance framework. Additionally, I will examine how these frameworks have been used in regulatory contexts.

Subproject 2: In this subproject I will have to understand how the consultants at Northwave conduct their assessments. This is critical for the system that I will be building to seamlessly integrate with their processes. I will have to interview some of the consultants, understand how they gather and process information, and how I could improve this. It might be necessary to adapt some of the processes and possibly introduce some new details into the assessments, to enhance the automation.

Subproject 3: This subproject will focus on designing an appropriate methodology for assessing NIS2 compliance. I will explore various ways to automate the compliance assessment process. This will involve identifying key elements of the assessment that can be streamlined through automation, such as analysis and reporting of the recorded interviews. I will evaluate existing tools and technologies, such as LLMs, to determine their suitability. Based on these findings, I will propose and prototype an automated solution that integrates into the broader compliance assessment framework at Northwave.
In the final subproject, I will implement and validate the developed framework and methodology, using automation wherever feasible. This will include testing the solution in collaboration with Northwave and refining it based on feedback from both the consultants and their customers.

1.3.1 Evaluation and Adjustment

Certain subprojects might raise challenges in information gathering, or in execution. The potential risks are presented below, together with a potential plan for handling them.

Subproject 2: Potential risks include the time needed to understand the internal processes within the consultant team. Additionally, scheduling meetings could be troublesome, as they are often busy with their customers. I will address this by establishing a core person within the team that I will reach out to for my project. I will plan all meetings at least 2 weeks in advance, so that I can stick to the time plan and not incur delay, in case the team is busy.

Subproject 3: A risk that may arise is the lack of resources on how reporting can be automated. In this case, I will rely on the expertise of my supervisor at the company to guide my methodology. I will also look for examples outside the cybersecurity field, in areas where certain methods might be transferable.

1.4 Timeplan and Milestones

In Figure 1, all milestones for the project, both internal and from SBP are listed.

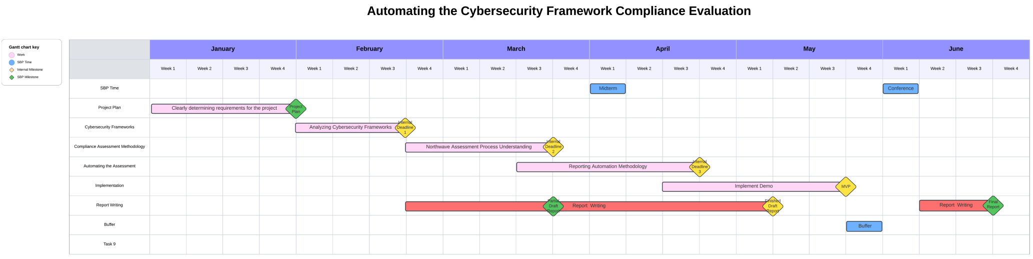

Figure 1: Gantt chart of the project time plan, including milestones. The chart can be seen in more detail here.

1.5 Educational Context

-

2 Scientific Foundation of the Project

2.1 Scientific Context

Cybersecurity is a growing concern for various organizations, ranging from large governmental bodies such as the EU, all the way down to SMEs that face a considerable number of attacks, 43% of the total, according to an Accenture report [6]. The same report states that the organizations at the forefront of cyber readiness and resilience make wide use of automation in their security processes. Northwave has set out on a similar path of identifying opportunities for automation, with many examples of successful projects. For example, their Security and Privacy Office now uses an LLM-based tool to triage and respond to e-mail phishing incidents. A recent survey of the field describes the way that LLMs specifically have been used in cybersecurity for automating various processes [7]. Some examples include gathering and processing Open Source Intelligence (OSINT) from unstructured sources, such as incident reports [8], and extracting information such as threat actor, attack type and timeline. This survey did not mention any literature works focused on automating cybersecurity governance, such as the reporting of a compliance assessment.
In the context of this growing research field, my project will strive to improve and speed up reporting processes, in order for Northwave to better help more organizations to get up to speed in their cybersecurity journey.

2.2 Literature sources

The first step in determining the direction of the project was searching for related literature. Initially, the search was focused on the cybersecurity field. The following search terms were combined to find literature: ”cybersecurity”, ”framework”, ”reporting”, ”automation”, ”LLM”, ”governance” and ”compliance”. The search failed to find any literature directly applicable to automating a compliance assessment report. Thus, the search was expanded to other fields, looking to include works where LLMs are used for summarization or reporting tasks.

Various papers employ LLMs for text-processing tasks, due to their ability to understand and generate human-readable text. A study was done on generating patient-friendly medical reports from radiology reports [9]. The goal of this system was to translate jargon-heavy medical reports into an understandable format for patients. The system designed by the researchers had a high success rate in producing understandable reports while maintaining complete medical accuracy and providing insight into the progression of the medical assessment. This was done to prevent unnecessary worry with patients misunderstanding the specialist's assessments and notes. This work is relevant to my project as it showcases the ability of LLMs to synthesize complex domain-specific information into easily digestible and actionable reports. The NIS2 regulatory framework emphasizes accountability with the higher management of the company. However, they are not directly in charge of information security, and the compliance assessment is usually done with technical parties at the company. LLMs could act as the glue between the technical aspects and the strategic implications, as they could be used to break down the technical jargon into language that executives can process and act upon.

A potential concern is the applicability of LLMs, which are trained on broad, generic datasets, in specific fields, such as cybersecurity. A study was done on creating a smart auditing system in the manufacturing sector, powered by LLMs [10]. In order to make the LLM more applicable and reduce the number of errors, the authors used a technique called Retrieval-Augmented Generation to connect the LLM to a domain-specific knowledge base, thus enhancing its reasoning capabilities. Since cybersecurity is also a domain where specific knowledge is needed, this technique could be applied to adapt a generic LLM for the task needed in this project.

2.3 Scientific Advisors

Name	Implication in the Project	Affiliation	Experience
Jair Santanna	Supervisor at Company	Northwave	Researching and implementing automation solutions for the processes at Northwave
Fadi Mohsen	Science Supervisor	RUG	Cybersecurity research and NIS2 expertise
TBD	Advisor	Northwave	NIS2 business consultancy towards customers of Northwave

Jair Santanna
As the supervisor of my project at the company, I will need to discuss with Jair how to implement automation successfully. He has experience in projects similar to mine and he can advise me on how to design the right methodology for the job. He can also provide insight into what cutting-edge methods could be useful when working with LLMs.

Fadi Mohsen
As my science supervisor, Fadi will advise me on the scientific side of my report. The concern that he will be able to address is the evaluation of the methodology and the potential prototype that I will build. Ensuring an accurate evaluation is necessary for contributing valuable results to the research in this field.

TBD
A soon-to-be-determined supervisor, part of the business consultancy team. I will require expertise from the consultancy side, to ensure that the reporting that the automated system creates is well done and matches the quality expected from Northwave. I will also need support from them to understand compliance requirements and how they should be handled in reports.

3 Societal Framework

3.1 Social Map

In Figure 2, a map of the stakeholders of the project is presented.

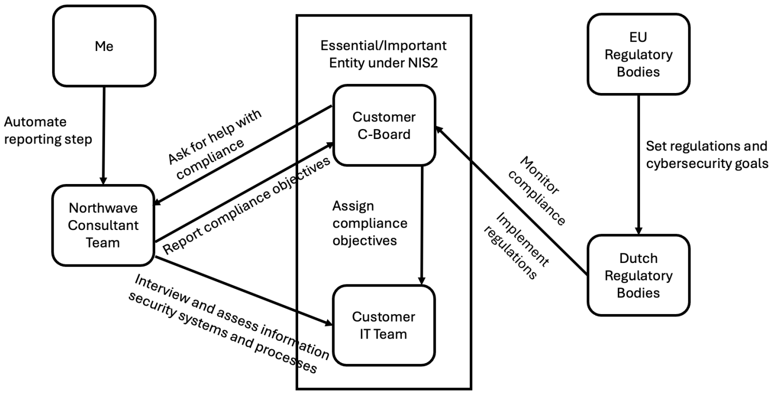
Me
Automate reporting step
Northwave Consultant Team
Essential/Important Entity under NIS2
Customer C-Board
Ask for help with compliance
Report compliance objectives
Assign compliance objectives
Interview and assess information security systems and processes
Customer IT Team
EU Regulatory Bodies
Set regulations and cybersecurity goals
Monitor compliance
Implement regulations
Dutch Regulatory Bodies

Figure 2: Social map of the project.

The Customer is the central entity representing the customers of Northwave that will benefit from my project. This is a company that falls under one of the two categories referenced in NIS2, essential or important. The company is split into two parts, which are both main stakeholders within my project. The first part, the C-level board is the upper management of the company. NIS2 aims to bring cyber security to their attention, thus also making them responsible for ensuring a high degree of information security. However, the board is responsible for strategic decisions and is not concerned with the implementation of cyber security measures. Thus, they assign this task to the technical employees at the company. They have to make sure that all processes and measures are implemented. To make sure that they are compliant, and to avoid any potential fines and damage to the company, the board hires Northwave to perform an assessment.

Northwave gathers information through interviews, documents, and sometimes hands-on investigation into the systems at the company. The consultant team consolidates all of this information and then creates a report with their findings. This report is meant both for the technical personnel, as well as the executive board. Thus, this report is very complex to create, due to the large amount of information it condenses and the dual audience. This process can be largely sped up through automation, which is what I will be investigating for Northwave.

EU regulatory bodies are the last stakeholders in the figure, that oversee the national regulatory bodies. It is the dutch authorities that are in charge of upholding the regulations when it comes to essential and important entities. Thus, they also hand out fines for failing to comply with regulations.

3.2 Ethical Aspects

Since I will be working on automating the reporting process of Northwave's assessments, two important ethical aspects need to be considered and investigated.

Accountability is often an issue when human tasks are automated. The responsibility for the result is shifted from the human to the machine/algorithm. But what happens when the algorithm is wrong?

In this case, the results could be dire. Companies rely on Northwave to assess their compliance with regulations that impose severe fines otherwise. Besides this, a missed weak link in the cyber security chain of a company could mean that attackers have a much easier time compromising the systems and causing loss of profit, data, or even life, in the case of critical infrastructure. I plan on considering these risks carefully, and ensuring that the system always remains under human supervision.

Quality can sometimes be a trade-off when leaving complex tasks to automation tools. Northwave has to uphold its reputation as a trusted and professional company, thus I need to ensure that the system I design produces results at least on par with the human consultants. Again, this can be ensured with human supervision.

3.3 Your role as a professional science advisor

As a science advisor, my role requires me to understand both the technical aspects of my project, as well as how it helps the business model at Northwave. For this, I will have to talk with many of the people at the company, as the project is fairly technical, but serves the consultancy department. I need to ensure that it is easy to use, helps them save time, and does not need constant adjustment and maintenance.
For this, I will make use of the expertise of my supervisors. I aim to have at least biweekly (possibly weekly) meetings with my supervisor at the company and at the university. In addition to this, I want to have regular meetings with my science supervisor and someone from the business consultant team.

Bibliography

[1] E. Union, “Critical infrastructure protection.”

[2] E. Union, “Nis2 directive: New rules on cybersecurity of network and information systems.”

[3] RVO, “Cybersecurity obligations for more companies in critical sectors (nis2).”

[4] ISO, “ISO/IEC 27001:2022 — iso.org.” `https://www.iso.org/standard/27001`, 2022. [Accessed 27-01-2025].

[5] C. Pascoe, S. Quinn, and K. Scarfone, “The nist cybersecurity framework (csf) 2.0,” 2024-02-26 05:02:00 2024.

[6] Accenture, “State of cybersecurity resilience 2023,” Jun 2023.

[7] M. Hassanin and N. Moustafa, “A comprehensive overview of large language models (llms) for cyber defences: Opportunities and directions,” 2024.

[8] F. Sufi, “An innovative gpt-based open-source intelligence using historical cyber incident reports,” *Natural Language Processing Journal*, vol. 7, p. 100074, 2024.

[9] M. Sudarshan, S. Shih, E. Yee, A. Yang, J. Zou, C. Chen, Q. Zhou, L. Chen, C. Singhal, and G. Shih, “Agentic llm workflows for generating patient-friendly medical reports,” 2024.

[10] X. Yao, X. Wu, X. Li, H. Xu, C. Li, P. Huang, S. Li, X. Ma, and J. Shan, “Smart audit system empowered by llm,” 2024.