Kristiania

Høyskolen Kristiania
Oslo, Spring 2024

NSM Grunnprinsipper for Enhanced ISO/IEC 27002 Compliance

A Framework Analysis and Implementation Impact Study

Berg, Bjerkseter, Evensen, Vatne, Walker

Supervisor: Stig Høyklint

BA302 - Cyber Security

Kristiania

Acknowledgements

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Oslo, Mai 2024

Oliver Berg

Erik Bjerkseter

Mats Evense

Henrik Vatne

Paul Walker

Contents

List of Figures

List of Tables

1 Appendix

2 Introduction

In an era where the digital threat landscape is on the rise, Norway's new Digital security law represents a significant move to strengthen national cybersecurity.

This recent legislation compels businesses to adopt the Norwegian National Authority's (NSM) "Basic Principles for ICT Security" (Grunnprinsipper for IKT-Sikkerhet) as outlined in the government's press release **Regjeringen** These guidelines serve as a foundational framework for enhancing cybersecurity across the nation

The Idea for our project came during our initial meeting with the client, They informed us that at this point they did not have a structured framework on which they were basing their cybersecurity around and that they intended to aim for an ISO 27001/27002 certification a goal that would both strengthen their defences but also enhance their credibility in the industry.

Understanding the complexity and resource demands associated with achieving ISO certification, we recommended beginning the structured approach by adopting the Norwegian National Security Authority's (NSM) "Basic Principles for ICT Security" (Grunnprinsipper for IKT-Sikkerhet).

Our role involved guiding the client through the implementation of the NSM's grunnprinsipper, providing them with tailored, step-by-step assistance. Early on, it became apparent that the client found many of the principles challenging to understand due to their technical complexity.

Recognizing the challenges faced by our client and similar small to medium-sized businesses (SMBs), we identified an opportunity to create a more user-friendly version of the NSM principles. This adaptation aims to make these foundational security principles more accessible and understandable, especially for teams without extensive technical expertise in cybersecurity. By simplifying the guidelines, our project seeks to meet the specific needs and constraints of SMBs, facilitating easier adoption and compliance with cybersecurity measures. This approach not only aids our client in building their cybersecurity capacity but also aims to help other SMB's.

Implementing the simplified NSM principles and working towards ISO certification could have significant implications for operational security and business development. By adopting these guidelines, our client and similar businesses may be better positioned to enter new markets that require strict cybersecurity protocols. This adaptation also has the potential to streamline

business processes, which could reduce the risks and operational disruptions associated with cyber incidents. In turn, these improvements might enhance trust and reliability among customers and stakeholders, possibly leading to stronger business relationships and new opportunities for revenue generation.

3 Background

3.1 The Client

Respecting the desire for confidentiality by our client, they will hence be referred to as the client. The following is a brief description of the client and their background, as provided by the client themselves:

> *The Company is a distinguished manufacturer of high-quality products integral to the industrial chain and, ultimately, the the global construction industry, amongst others. With a workforce of approximately 250 employees, the Company operates through a network of production facilities. Recognizing the importance of enhanced security, the The company is committed to elevating its standards by adhering to the 'NSM's grunnprinsipper', ISO 27001, and NIS2 directives.*

Given the client's industry and the nature of their operations, their The IT department is rather small, consisting of only a few employees. This means that the client has limited resources to dedicate to the implementation of an ISMS. As such, the client is seeking external assistance to help them develop and implement the necessary security policies to meet the requirements of the NSM's grunnprinsipper, ISO 27001, and NIS2.

3.2 Expected Outcome

Building on our assessment of the client's needs outlined in the previous chapter, this section delves into the specific outcomes we anticipate from implementing the NSM's grunnprinsipper as a foundational step towards comprehensive ISMS standards like ISO 27001 and NIS2.

Be om sitat her for hva Dynea vil ha som forventet utfall.

In this chapter we detail the expected outcomes that will come from out project with the client. The guidance we will provide the client in implementing NSM's grunnprinnsipper. This will include the creation of a wiki-based implementation guide that provides in-depth recommendations on implementing the basic principles of NSM.

The final product should be capable of being used as a standalone web application or integrated tool that can be used practically within the organization. By establishing this

groundwork, we aim to enhance the client‘s security measures and set a robust foundation for working towards a future certification.

1. Enhanced Comprehension: The guide will detail each principle with step-by-step instructions, enhancing the client's understanding and enabling them to implement these practices confidently and correctly.

2. Streamlined Implementation Process: Structured as a user-friendly wiki, the guide will serve as a comprehensive repository of information that provides practical examples and recommendations.

3. Scalability and Adaptability: As a universally adaptable tool, the guide can be updated and expanded to meet evolving security needs and new regulatory requirements, supporting the client's growth

3.3 Group Goal

As we sat down to plan our approach we decided to split our goals into two categories during the Bachelor theses. There are the business goals and our personal goals.

We had Initial meetings with the business to determine what goals they wanted to achieve through this project. Our personal goals were determined through an internal meeting where different members expressed what they wanted to learn and achieve.

Group goals

- Gain practical experience implementing security frameworks at a business.

- To create a User-friendly framework that is based on NSM‘s grunnprinsipper, to help smaller Norwegian businesses improve their cybersecurity capabilities.

Business Goals

- The product will increase the business capabilities of cyber security and improve resilience towards potential attacks.

- The documentation is to be written in English so that it can potentially be used throughout the business group.

- To find potential gaps in the security and find ways of improving upon them.

- Getting closer to the ISO27001 Certification

3.3.1 Target Group

NSM released these principles as a general recommendation, but they are somewhat challenging to understand for non-technical leaders. The target group for this project is small and medium-sized businesses, as they often experience limitations regarding resources and capabilities. Some principles are more technical and hard to understand for business owners and non-technical leaders. These leaders carry the ultimate responsibility for their business, and therefore, we want to help them with understandable cybersecurity guidelines and help them grasp the fundamentals. This understanding will help them make more informed decisions and allocate their resources effectively by understanding the trade-offs involved in cybersecurity choices. It will also help bridge the gap between leadership and the IT team when communicating needs and risks. We would like to present two primary and one secondary target group for our intended product as that these groups could benefit deeply from our product.

Group	**Purpose**
Primary	Businesses that either intend to strengthen their overall cybersecurity posture or work towards ISMS certifications.
Secondary	GRC Professionals consulting with ISMS certifications.

Table 3.1: Target Groups

The document is very technical, and it can be hard to understand all the points without an IT background. It lacks definitions and specifications for technical-related terms, and some hyperlinks are outdated and no longer work. These links would clarify some cases, but having a more available framework would be easier, and the user wouldn't have to use additional resources to understand technical terms, explanations, or definitions.

We would eventually learn that NSM was looking to update their document the same year to a 2.1 version with updated working links and a version in English. The product will contain more information than the original document but will be simplified and more user-friendly. The markdown sheets allow us to easily link pages between them and internal linking towards definitions, explanations, tool suggestions, and even templates for that principle.

4 Analysis and design

4.1 Requirements for the solution

Define the boundaries and applicability of the ISMS, including which parts of the organization it will cover.

The scope of the implementation of the ISMS was discussed early in the process of our partnership. Only part of the organization was going to take on this implementation. The client wanted to focus on the IT infrastructure which where used for all the office work. This includes internal and external devices such as desktops, laptops, phones, servers, databases, and USB hard drives. Other parts of the organization related to operational technology (OT) include hardware and software systems that monitor and control physical processes and equipment was not included in our project because of security reasons.

5 Project Management

5.1 Methodology

Project management frameworks generally adhere to either a traditional or agile approach. Traditional methods follow a linear structure where a category of tasks should be completed before starting a new one. In contrast, agile methods prioritize constant feedback, adaptability, and flexibility in a holistic approach to the project, allowing for simultaneous progress toward the ultimate goal. Weighing our former experiences with project work, the team concluded that implementing a reliable and established development framework would provide the necessary coherence for our upcoming project.

A collective decision was made to use "Scrum," an agile framework that offers excellent flexibility and is suitable for our sought-after qualities. By focusing on short development cycles (sprints) lasting upwards of a month, Scrum helps stay on track toward achievable near-term goals (Rubin, 2012). This approach would enable adaptability when faced with altering requirements and receiving regular feedback from the product owner. We decided on Scrum as the methodology aligns with our goals, facilitating a shared perception of responsibilities and accountability towards the group meeting sprint objectives. We facilitated streamlined task management by implementing Trello as our backlog. The platform offered exceptional transparency, letting all members stay updated on the project's progress and upcoming assignments. We dedicated the first two weeks of our project to meticulously planning and establishing backlog by identifying what we perceived to be fundamental steps for the process ahead. By initiating the working phase of our project upon this foundation, we could continuously keep a relevant backlog outlining our development process and identifying and prioritizing tasks.

Before a sprint, the team determined which tasks to tackle during the coming week. We then attempted to adhere to the Scrum framework, assigning each member roles. The Scrum Master facilitated the process, while the external supervisor was the Product Owner. We held daily standups and bi-weekly Scrum meetings to review completed tasks, plan upcoming objectives, and address any challenges. The approach improved our team's accountability and ensured smooth project progression.

5.2 Tools and Services

To facilitate smooth collaboration, our process adapted and implemented a series of tools. Choosing for their respective strengths, these tools became essential in providing a structured environment, allowing for a flexible and efficient workflow.

5.2.1 M365 Suite

Through the initial stages of working with the client, we rapidly identified the need for a more structured system to facilitate the implementation of the NSM's grunnprinsipper. The client's current approach to managing security policies was fragmented, with policies stored in various locations and formats. This made it difficult to maintain an overview of the organization's security posture and ensure that policies were up-to-date and accessible to all relevant stakeholders. A template to be used for all security policies was proposed to address this challenge at an initial stage. The template would provide a consistent structure for all policies, making maintaining and updating them easier. We also recommended using a document management system to store and manage the policies, ensuring they were easily accessible to all relevant stakeholders. As a starting point, the client wanted to keep the implementation within the M365 environment. Teams were employed to share documentation, conduct meetings, and uphold communication between the client and our team. In preparation for weekly meetings between our group, the IT department, and their Product Owner, team members prepared documents w/material to be reviewed and worked on throughout the coming session. These documents followed an easy template structure for authoring and documenting internal data to become relevant for further certification revisions.

The templete, as visualuzed in Table 3.1 was developed to accommodate the client's needs and to ensure that all relevant information was included in the documentation. The template was used to structure the documentation, ensuring all relevant information was included and the document was easy to navigate. The template was also used to ensure that all documents followed the same structure, making it easier to find information.

Forfatter		NSM tiltak ID	
Revidert dato		ISO/27002 ID	
Godkjent av			
Kategori			
Grunnprinsipp			
Beskrivelse			

Table 5.1: Basic Template

5.2.2 Workspaces

Google Workspaces facilitated internal collaboration. A highly effective measure as it offers high adaptability for custom workflows, the ability to share documents, conduct meetings, and uphold communication between team members. The platform was especially useful as it allowed for real-time collaboration on documents, ensuring that all team members were working on the most recent version of the document.

5.3 Source Control

It was necessary to implement a standardized system for source control that that would be universally adapted on all repositories consisting of markdown, code, and tex files. We utilized Git and GitHub for this purpose. This allowed multiple team members to work on different project sections simultaneously without the risk of overwriting each other's work. Implementing a version control system was essential to keep track of changes made to the documents and ensure that all team members were working on the most recent version. This was especially important as the project progressed and the documents became more complex.

5.4 User Testing

The goal behind our initiative towards revising NSM is to enhance cybersecurity capabilities within the Norwegian business sector. A user testing method was employed to gain insight into how our approach is perceived and used. This involved working with a sample group of Norwegian businesses representing the framework's target audience. The user testing group came from other businesses under the same holding group as the business we are working with. The feedback we were given helped shape our final product, as none of the members in the group had a design background, which helped finish off the end product in a positive manner.

Our ISMS management system, built upon the NSM framework, simplifies cybersecurity for Norwegian businesses. We focused on creating a design centered around the user's needs, knowing that a framework only works well if it's easy to access and fits the business it's meant for. We aim to help Norway's businesses stay secure in a way that makes sense.

6 Proposed Solution

6.1 Background

The driving factor behind our proposed product is our goal to improve the accessibility of NSM-GP. At the beginning of this project phase, we experienced collective fatigue from attempting to tackle such a severely theoretical and subjectively structured framework. As we developed techniques for easing the content and providing a clearer structure, we realized that such a product could benefit not only our client but also additional organizations in their early stages of ISMS work.

The idea is simple: we aim to break down the official version grunnprinsipper into descriptive and clear "pages" containing necessary principle data, its relations, and supportive material explaining the contents. Following the official structure of grunnprinsipper where, there are four main categories, each containing a number of principles with several corresponding measures, we will provide an intuitive and easy-to-navigate system acting as both a guide to the principles but also a sort of an encyclopedia for the client to use in their daily work.

6.2 The Product

Central to our product is a repository of markdown files containing structured data from the NSM-GP PDF. Markdown is a simple text format that is universally adaptable as it is not built on top of proprietary technology. This allows for a basic, but really capable file system that can be applied and customized for different use cases.

7 Discussion

8 Conclusion

Appendices

A Test

Figure A.1: Kristiania logo