PM: Information Security Management System

Carina Bengtsson and Lennart Franked

21 mars 2022

1 Introduction

This assignments focus on information security management systems (ISMSs). The purpose of an ISMS is to manage an organizations work within the field of information security.

2 Aim

This assignment aims to:

- To give you an understanding of the importance of an ISMS.
- That you will be able to evaluate what information is important to have in an ISMS.
- That you are able to account important success factors to be able to implement an ISMS.

3 Reading assignment

Before starting this PM, you should have read the following documents:

- *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter* [1]
- *Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018)* [2, chap. 4] (Use as a support document only, if you don't understand Swedish, use this as the main reference)
- *Introduktion till metodstödet* [3], och
- *Ledningens engagemang avgörande* [4]

Alternatively

- ISO 27000 standard [2, Chapter 4]

4 Task

This assignment contains four sub tasks, One introduction task covering ISMSs, including Swedish statutes, success stories and how to get a committed leadership.

4.1 Information Security Management System

Shortly describe a management system is, and more specifically what an ISMS is. Your description should also cover how an ISMS is structured.

4.2 Legal requirements according to MSBFS 2020:6

In an ISMS, there are certain work tasks defined for the organisation. The Swedish Civil Contingencies Agency (MSB) have defined in their statutes MSBFS 2020:6 [1], which is binding for governmental agencies, stated that the governmental agencies should:

1. Ensure that there is an information security policy where the management's objectives and focus on the information security work are shown,
2. Clarify the management and the rest of the organizations responsibilities, including the person or persons appointed to lead and coordinate information security work, and give these positions the powers needed,
3. ensure that the information security work is assigned the necessary resources,
4. establish the necessary internal rules, working methods and support
5. ensure that the content of the organisation's internal rules, working methods and support is evaluated and, if necessary, adapted.

Further more, in 14§ that

6. the management should keep itself up to date with the work with information security, and at least once a year do a follow-up and evaluate the information security work.

Shortly reflect around the key points 1, 2 and 3, *then* select one of the key points 4, 5 or 6.

If you are using the English course material, refer to the key-points a-i in [2, chap. 4.2.1]

Write down why you think each of the requirement is important, or not as important to incorporate in an organisation.

Note that the organisation does not necessarily need to be a governmental agency.

4.3 Success factors

To implement an ISMS in an organisation is a large project. Therefore the material mentions some success factors that are critical to achieve a successful implementation [2, s. 4.6]. Give a short summary about these success factors.

4.4 Commitment from the Management

If you where put in the position to try to convince the management in a company to implement a an ISMS. How would you motivate them?

5 Examination

This assignment will be examinated through a written PM that will be handed in as a PDF-document. The PM *must* must cover the tasks from avsnitt 4:

1. Information Security Management System;
2. Requirements according to MSBFS 2020:6, points 1–3 and one of the following key points 4–6. Or if you are using the english material, key-points a-c and one the points d-i in [2, chap. 4.2.1].
3. Success factors; and
4. Commitment from the Management

Your PM should be written with an academic language in either english or swedish. It must contain correct references.

Referenser

[1] *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet*. MSBFS 2020:6. URL: `https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20206/`.

[2] *Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2018)*. Standard. Available through University Library. Stockholm, Sweden: Swedish Standards Institute, febr. 2020.

[3] *Metodstödet*. Hämtad den 21 mars 2022. Myndigheten för samhällsskydd och beredskap, 2018. URL: `https://www.informationssakerhet.se/metodstodet/metodstodet/`.

[4] *Ledningens engagemang avgörande*. Hämtad den 21 mars 2022. Myndigheten för samhällsskydd och beredskap, 2018. URL: `https://www.informationssakerhet.se/metodstodet/anvanda/#ledningens-engagemang-avg%C3%B6rande`.