

Cybersecurity: Technology and Governance

Audun Jøsang
1st edition 2024
Springer Nature



Exercises

Chapter 18: Cybersecurity Governance

Exercise 1: Information security standards

- Look at the list of standards in the ISO 27000 series, for example:
<https://www.iso27001security.com/>
 - View the NIST SP800 (Special Publications) series at:
<https://csrc.nist.gov/publications/sp>
- a. Try to identify similar standards in the ISO 27000 series and in the NIST SP800 series.
 - b. What might be reasons for different organizations to develop separate similar standards?

Exercise 2: ISMS

- a. How are the ISO/IEC 27001 and ISO/IEC 27002 standards related?
- b. What does "system" mean in the abbreviation ISMS (Information Security Management System)?
- c. Which of the above standards forms the basis for certification, and why?
- d. How should an organization determine which security controls to implement?

Exercise 3: SoA – Statement of Applicability

- a. What is Annex A in ISO/IEC 27001?
- b. What is a SoA (Statement of Applicability)?
- c. A company wants to use a different repository of security controls than ISO/IEC 27002 to choose information security controls. Assume that the enterprise wants to use NSM's Basic Principles for ICT Security. What does the company need to do to prepare a SoA?

Exercise 4: Information security controls

Detailed security controls under each principle of the NSM guidance are available from:
<https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/>

- a. How can the effectiveness of security controls be measured?
- b. Below is an example of a security control under the principle: *"Have control over identities and access"* from the NSM guidance.
Action 2.6.7: *"Use multi-factor authentication, such as smart cards, certificates, or one-time passwords, to authenticate users."*
Suggest methods to measure the effectiveness of this control.

Exercise 5: ISSG – Information Security Steering Group

An Information Security Steering Group (ISSG) (or Information Security Committee) is important to ensure the quality and maturity of the ISMS.

- a. What composition should the ISSG have?
- b. What tasks are appropriate for ISSG?

Exercise 6: The Cyber Defense Matrix

Explain how the cyber defence matrix can be used for gap analysis, i.e. to show what security controls the company has, and what security controls the company wants to implement for different assets and security functions.