University of Oslo
INF3510 Information Security
Spring 2010
Workshop Questions

Lecture 11: Security Management and Secure Systems Development

The standards ISO/IEC 27001 and ISO/IEC 27002 are available to UiO students online via the INF3510 wiki pages https://wiki.uio.no/mn/ifi/INF3510/. You need to use your UiO logon to access the wiki pages.

QUESTION 1

Using the lecture slides, review the roles and responsibilities for each of the following groups of people with regard
to information security management in any organization.
(a) Management
(b) General security staff
(c) IT staff
(d) Users
(e) Third parties

QUESTION 2

a. How are the standards ISO/IEC 27001 and ISO/IEC 27002 related?
b. Which one of the standards can be used for certification?
c. Mention a certification body in Norway.

QUESTION 3

Briefly and clearly explain the PDCA model applied to ISMS processes.
Plan - Do - Check - Act model outlined on page v of ISO/IEC 27001.

QUESTION 4

Read through Section 5 Security policy in ISO/IEC 27002.
a. Briefly explain the main objective of the information security policy
b. Who should read it?
c. Where should it originate?
d. What should happen to it after it is produced?

QUESTION 5

The article “10 Deadly Sins of Information Security” by von Solms and von Solms published in 2004 is available on the INF3510 website. The 10 deadly sins are listed below.

1. Not realizing that information security is a corporate governance responsibility (the buck stops right at the top).
2. Not realizing that information security is a business issue and not a technical issue.
3. Not realizing that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single ‘off the shelf’ solution).
4. Not realizing that an information security plan must be based on identified risks.
5. Not realizing (and leveraging) the important role of international best practices for information security management.
6. Not realizing that a corporate information security policy is essential.
7. Not realizing that information security compliance enforcement and monitoring is essential.
8. Not realizing that a proper information security governance structure (organization) is essential.
9. Not realizing the core importance of information security awareness amongst users.
10. Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities.

Answer the following questions about these “10 deadly sins”.

a. Suppose a company has established an ISMS following ISO/IEC 27001. For each of these 10 potential sins, identify the place or places where they are addressed in the ISO/IEC 27001 document. Hence decide whether ISO/IEC 27001 can be used to prevent companies from committing any of the sins.
b. Section 0.7 of ISO/IEC 27002 lists 10 critical success factors in implementing information security in an organization. Try to provide a mapping between each of these success factors and the 10 deadly sins; in other words find out if each success factor corresponds to avoiding one or more of the deadly sins.
c. How can ISO/IEC 27002 play a role in avoiding the sins? ISO/IEC 27002 details the controls that can be used as part of implementing an ISMS.

QUESTION 6

SDL (Security Development Lifecycle) is a development maturity model for security used by Microsoft.

a. What are the steps of SDL?
b. In which step is risk analysis done?
c. What is a buffer-overflow vulnerability?
d. In which step are techniques used to prevent or discover buffer overflow vulnerabilities on software?
e. Security usability is a desirable property of security applications, whereby users can easily understand and operate security functions. Which steps of the SDL are important for security usability, and why are they important?