University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 2: Security Management, Human Factors & Physical Security

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

What are the responsibilities for each of the following groups of people with regard to information security management in any organization.
(a) Management
(b) IT Security staff
(c) General security staff
(d) IT staff
(e) Users
(f) 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

a. What is a social engineering attack? See e.g SANS InfoSec Reading Room on Social Engineering (http://www.sans.org/rr/whitepapers/engineering/).
b. Describe three typical social engineering attack strategies.
c. What are the elements of David Gregg's *"Multi-Level Defence Against Social Engineering"?*

QUESTION 6

Access control mechanisms fall into one of two categories: physical or logical.

a. When is physical access control not enough or not possible?
b. Give three examples of physical access control mechanisms.
c. What is meant by a multilayered approach to physical access control?

QUESTION 7

Explain the main characteristics of the following UPS types:

a. Standby or offline UPS
b. Ferro-resonnant standby UPS
c. Line-Interactive UPS
d. True Online UPS

QUESTION 8

a. What does the abbreviation CPTED stand for?
b. How does CPTED work?
c. Which are the main principles used in CPTED

QUESTION 9

a. Create a mapping of the correspondence between the 11 security domains of ISO27002 and the 10 security domains of CISSP.
b. Make a judgment about how well aligned they are.
c. Mention security topics that you think are missing in one or the other.