University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 13: Privacy and Regulatory Requirements

QUESTION 1

The Basel II agreement is important for the financial sector.

a. Briefly describe the purpose of Basel II, and when the first version was published.
b. What is needed to make Basel II mandatory for banks?
c. Basel II specifies requirements for both operational risk and credit risk. Mention 3 specific areas of operational risk described by the Basel II agreement that are relevant for information security.

QUESTION 2

There are several laws regulating electronic and digital signatures around the world.

a. What is the relevant EU directive called, and when was it published?
b. What is the goal of the EU directive?
c. What is the corresponding Norwegian law called (in Norwegian or English), and when was it published?
d. Which evaluation assurance level is required of equipment to produce “advanced signatures based on qualified certificates”.

QUESTION 3

a. When did the OECD issue its guidelines on data privacy protection?
b. When did the EU publish the Data Protection Directive
c. When came the first data privacy act in Norway, and what was its name?
d. When came the current data privacy act in Norway and what is its name?
e. Briefly describe the purpose of the “US-EU Safe Harbour Program”.

QUESTION 4

The OECD guidelines specifiy a set of principles for the protection of personal data.

a. Explain the *Security Safeguards Principle*.
b. Explain the *Individual Participation Principle*.

QUESTION 5

In addition to the Data Protection Directive, the EU has issued two more directives that are relevant for privacy.

a. What is the goal of the E-Privacy Directive (Directive 2002/58/EC)
b. What is the goal of the Data Retention Directive (Directive 2006/24/EC)
c. In case of conflict between laws based on the Data Protection Directive and the Data Retention Directive, which will normally carry the most weight, and why?