



## ***Lecture 12: Privacy and Regulatory Requirements***

### **QUESTION 1**

The Basel II agreement is important for the financial sector.

- Briefly describe the purpose of Basel II, and when the first version was published.
- What is needed to make Basel II mandatory for banks?
- 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.

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

### **QUESTION 3**

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

### **QUESTION 4**

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

- Explain the *Security Safeguards Principle*.
- 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.

- What is the goal of the E-Privacy Directive (Directive 2002/58/EC)
- What is the goal of the Data Retention Directive (Directive 2006/24/EC)
- 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?