Name: __________________________________________________________

Read the questions carefully and answer four of the five questions. Be as precise and as concise as possible. You can consult your book or notes, but all work must be your own. Please write legibly and organize your answers carefully.

Please indicate here ______ which of the five questions you did not answer.

1. (10 points) We discussed four strategies for dealing with risk: avoid, transfer, mitigate, accept. For each of these explain what it means and give an example.

2. (10 points) One response to the discovery of an ongoing attack is called containment. A possible containment strategy is to “cut the link.” Explain what this means and discuss the pros and cons of this strategy.

3. (10 points) Firewalls are a common approach to perimeter defense. Explain packet filtering firewalls and discuss whether or not they provide good perimeter defense.

4. (10 points) Explain why employees constitute one of the greatest threats to information security?

5. (10 points) An intrusion detection system (IDS) is said to be accurate if it yields no false negatives. It is said to be precise if it reports no false positives.

(a) Discuss the following assertion: It is easy to make an IDS that is either accurate or precise, but hard to do both simultaneously.

(b) Discuss the relative importance of accuracy and precision for an IDS.