CPEN 442, Fall 2015 Key

Quiz #1

Your Family name: _____

Your Given name: _____

Your student ID: _____

Your CPEN 442 alias: _____

_____

#	Points	Out of
1		8
2		6
3		5
4		2
TOTAL		21

Notes:

- Make sure your handwriting is legible. If the teaching staff does not understand what your wrote, they mark your answer as if the unreadable text is missing.

- Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.

- As in real world, stated questions and/or accompanied descriptions in this quiz are often open-ended and one has to make assumptions in order to answer them. If you do make assumptions, state them clearly and explicitly.

- Don't panic if you feel like you are severely short on time. Everybody is. ☺

1. **(8 point) What can be done with risks (1 point for naming each)? For each of the approaches, provide an example (1 point for example per approach).**

a. Avoid - not use technology to avoid all risks associated with it. E.g., do not use online banking.

b. Transfer – transfer responsibility and risks to someone else. E.g., buy insurance for identify theft in online banking scenario.

c. Reduce – Install appropriate malware detection software to avoid phishing websites.

d. Accept – Just accept the risk of identity theft while using online banking and keep using it.

2. **(6 points) Explain CIA abbreviation (1 point per letter). Provide an example per letter (1 point for an example per letter)**

a. Confidentiality – Only authorized persons should be able to see data.
b. Integrity – Only authorized persons should be able to modify data.
c. Availability – Data should be always available to authorized persons.

3. **(3 points) In 2014 Canadian Revenue Agency got attacked through Heartbleed vulnerability (see handout on the last page for more details). Some information has been extracted. Discuss this attack from all CIA properties (3 points). Who are the stakeholders under attack in this event? (2 points)**

Confidentiality – Taxpayers data has been leaked. Private key SSL/TLS might have leaked as well.
Integrity – Not compromised that much (No evidence that something got changed surfaced)
Availability – Taxpayers were not able to submit their taxes while the service was offline.

Stakeholders:

1. **CRA**
2. **Tax-Payers**
3. **OpenSSL developers.**
4. **Solis-Reyes**
5. **Other possible, but not crucial.**

4. **(2 points) Which of the following <u>significantly reduces the risk</u> of legal actions against you, if you are performing penetration testing of an online system run by the administration of the City of Vancouver? Check any applicable.**
    a. **The fact that you are doing this analysis for a UBC course.**
    b. **The fact that it's a system operated by the local government.**
    c. **The fact that your intent is benign.**
    d. **The fact that you don't own substantial assets and therefore cannot repay the damages claimed by the City of Vancouver, in case the court makes such an order.**
    e. **The fact that you have not agreed to any terms of use for the system you are analyzing.**
    f. **The fact that you are following the process of responsible disclosure.**
    g. **The fact that you have discovered serious vulnerabilities, and it's in the best interest of the public to be informed about them.**

None of the options.