SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Tutorial questions for Lecture 4: Security management

Attempt these questions before you attend your tutorial/workshop session, and bring your prepared answers with you. Come prepared to discuss your answers and/or any problems you encountered in trying to answer these questions.

Much of this workshop material requires reference to Australian Standards documents. **The standards AS/NZS 27001:2006 (ISO/IEC 27001:2005), AS/NZS 27002:2006 (ISO/IEC 27002:2005) and AS27005:2012 (ISO/IEC 27005:2011) are available free to QUT students online via the Library***. From the Standards link on the library homepage, find the SAI Global – Standards Online (formerly Standards Australia Online) database. Enter the Australian standard number or title in the search box.*

NOTE: QUT has a limited number of concurrent licences (5). If all licences are in use, the system will return an error message and you will need to try again later (so don't leave your attempt at these questions until the hour before your class). If you are browsing particular Standards documents, it is best if you **download the document, then log out of Standards Australia and browse your saved local version**. This provides others with an opportunity to access Standards documents also.

QUESTION 1

Use the Australian Standard AS27005:2012 Information Security Risk Management to answer the following questions:

a) List, and give a clear and concise explanation of, the main elements of the information security risk management process. Figure 2, on p8 of AS27005:2012, is a useful diagram to accompany your explanation.

b) How are the terms `consequence' and `likelihood' defined in AS27005:2012 (Hint: See Clause 3, Terms and definitions)?

   i. Both of these terms may be determined quantitatively or qualitatively. Explain the difference between quantitative and qualitative expressions of consequence and likelihood.

   ii. For both consequence and likelihood, give an example of a scale for each type (quantitative and qualitative).

c) What is meant by the term `stakeholder' (Hint: See Clause 3)?

d) In establishing the context within which information security risks must be managed, the organization should define the scope and boundaries for the information security risk management process. What information should be considered when defining the scope and boundaries (Hint: See Clause 7.3)?

e) Clause 8 of AS27005:2012 deals with Information Security Risk Assessment.

   i. List the three steps that comprise risk assessment.

   ii. Give a brief description of each of the three steps; noting the required inputs, actions and outputs.

f) Clause 11 of AS27005:2012 deals with communication and consultation.

   i. What sort of information should be communicated?

   ii. Explain why communication and consultation are important, particularly with respect to stakeholders.

QUESTION 2

AS27001:2006 promotes the adoption of a process approach to an organisation's ISMS. Refer to the Standard document to answer the following questions:

a) Clearly explain the meaning of the phrase 'process approach' (See Introduction Clause 0.2).

b) What sort of organisations is the standard intended to apply to (Hint: See Clause 1)?

c) Which requirements must be met in order to claim conformity with this standard?

d) The PDCA model adopted in AS27001:2006 to structure Information Security Management Systems processes has four stages. Name each stage, and outline the processes involved in each stage (Summary in 0.2, Details in 4.2).

e) According to Clause 5, how should management demonstrate commitment to information security?

QUESTION 3

AS27002:2006 provides guidelines for effective information security management practices. Read through Clause 5 *Security policy* in AS27002:2006, and use this to answer the following questions:

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?

e) Locate the Information Security Policy for QUT. Is it consistent with these guidelines?

QUESTION 4

a) How are the standards AS27001:2006 and AS27002:2006 related?

b) Which one of the standards can be used for certification?

c) There are around 100 organizations in Australia with this certification. What assurance does the fact that these organizations hold this certification provide?

QUESTION 5

Suppose the risk management process performed by company ABC produced the following information regarding threats associated with their internet connection:

Threat to asset	Cost per incident ($)	Annualized Rate of Occurrence
Unauthorized access to internal information	100,000	0.02
Unauthorized use of computing facilities	10,000	0.30
Data corruption due to malicious code	50,000	0.05

a) Use the information about the threats recorded in the table above to determine the Annualized Loss Expectancy (ALE) associated with each threat event.

b) How much can justifiably be spent on controls to address this risk to the ABC company (if the risk criteria is financial)?

c) Which Information Security Standard provides some guidance on the sort of controls the company could consider applying to treat the risks?

d) From this standard, what sort of controls do you suggest that ABC consider?

QUESTION 6

Read the following news story concerning the data breach at Target US in 2013:

http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Use the information from the story to answer the following questions:

a) How did the data breach occur?

b) What sort of data was compromised?

c) How did the timing of this attack contribute to its success?

d) Did Target have any control measures in place to detect this type of security incident?

e) In the standard AS27002:2006, Clause 13 deals with information security incident management. Which aspects of this clause are relevant to the Target case? Justify your answer.

QUESTION 7

Read the Oct. 2010 Report 'The Billion Dollar Lost Laptop Problem' available at: http://www.intel.com.au/content/www/us/en/enterprise-security/enterprise-security-the-billion-dollar-lost-laptop-problem-paper.html. Answer the following questions based on the information contained in the report:

a) How many organizations were involved in the study?

b) Considering the average number per organization, in the 12 month reporting period, how many laptops:

   i. did each organization have?

   ii. were lost or stolen?

   iii. were recovered?

c) The report based the cost calculations for a lost laptop on the results of a previous study finding (from 2009) that the average cost of a lost laptop (in US$) was $49,246. List the seven cost components the researchers used to derive this cost figure.

d) What was the greatest cause of laptop theft?

e) What proportion of the lost or stolen laptops contained confidential data?

f) Table 5 presents calculations for the average cost of a lost laptop which is not encrypted, and the average cost for a lost laptop which is encrypted. What are the cost estimates in each case, and how do they differ?

g) How could these figures be used to inform information security risk management decision making? (Hint: Consider the cost of implementing controls compared to the potential reduction in loss achieved).