SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Outline solutions for

Week 5 tutorial questions for L4: Security management

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.

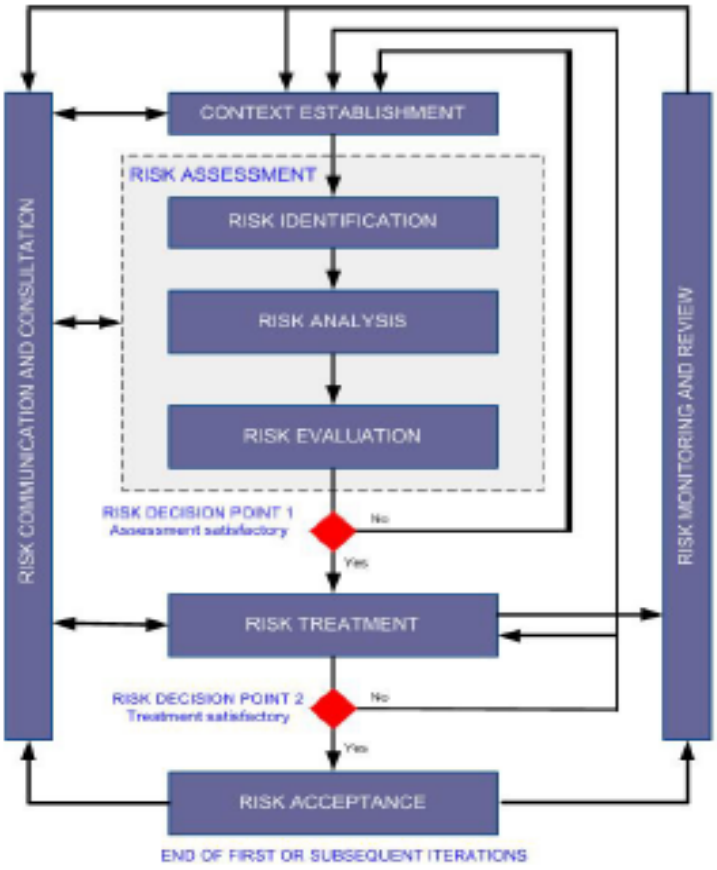
   ii. Give a brief description of each of the three steps; noting the required inputs, actions and outputs.

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.

a) **Main elements of the information security risk management process are outlined in Clause 6 *Overview* and shown in Figure 2 of AS21005:2012.**
    a. **Establish the context -external, internal and risk management context**
    b. **Risk Assessment:**
        i. **Identify risks - where, when, why and how events could prevent, degrade, delay or enhance the achievement of objectives**
        ii. **Analyse risks - Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk.**
        iii. **Evaluate risks - Compare estimated levels against pre-established criteria and balance potential benefit and adverse outcomes.**
    c. **Decision Point: If risk assessment is insufficient, return to Risk Assessment. Otherwise continue:**
    d. **Risk Treatment –**
        i. **Assess risk treatment**
        ii. **Decide whether residual risk levels are acceptable**
    e. **Decision Point 2: If risk levels are not acceptable repeat Risk treatment step for a new treatment, otherwise continue**
    f. **Communicate and consult across the whole process - with internal (appropriate managers and operational staff) and external stakeholders (could include public relations here)**
    g. **Monitor and review across the whole process - important for continuous improvement, and to ensure that changing circumstances do not alter priorities.**



b) Consequence: outcome of an event affecting objectives. Likelihood: chance of something happening.

- **i. The main difference between qualitative and quantitative expressions is that qualitative uses words to describe the magnitude of potential consequences and likelihoods, whereas quantitative uses numerical values.**
- **ii. Qualitative scale for**
  - **I. consequence could be: minor, moderate, major and**
  - **II. for likelihood could be: unlikely, likely, highly likely**
- **iii. Quantitative scale for**
  - **III. consequence could be: repair/replacement cost in dollars, and**
  - **IV. for likelihood use numerical probability values: 0, 0.1, 0.2, …, 0.9, 1.0**

c) A Stakeholder is defined as a `person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity'.

d) Scope and boundaries: According to Clause 7.3, consider

- **Business strategies, objectives and policy;**
- **Business processes;**
- **Organization's structure and functions;**
- **Legal, regulatory and contractual obligations;**
- **Organization's information security policy;**

- **Organizations approach to risk management;**
- **Information assets;**
- **Location of organization and geographical constraints;**
- **Other constraints;**
- **Stakeholder expectations;**
- **Sociocultural environment;**
- **Interfaces (for information exchange)**

e) **<u>Risk Assessment</u>: the overall process of *risk identification, risk analysis and risk evaluation*.**

<u>Risk identification</u>: the process of determining what, where, when, why and how something could happen

***Input*: Scope and boundaries, list of assets owners and users, locations, functions, possible threats, documentation for existing controls and treatment plans, known vulnerabilities related to assets,**

***Output*: Lists of assets, threats, vulnerabilities and incident scenarios with consequences related to assets and business processes.**

<u>Risk analysis</u>: systematic process to understand the nature of, and to deduce the level of risk

***Input*: List of identified relevant incident scenarios with consequences related to assets and business processes, and existing and planned controls.**

***Action*: Determine business impact on organization resulting from information security incidents, and likelihood of such incidents**

***Output:* List of risks with values assigned**

<u>Risk evaluation</u>: process of comparing the level of risk against risk criteria

***Input*: List of risks with value levels assigned, and risk evaluation criteria.**

***Action*: Compare risk levels with risk evaluation and risk acceptance criteria.**

***Output:* List of prioritized risks.**

f) **<u>Communication and consultation</u>: information to communicate includes the existence, nature, form, likelihood, severity, treatment and acceptability of risks. Communication and consultation are important to ensure that those responsible for implementing risk management and those with a vested interest understand the basis on which decisions are made, and why particular actions are required.**

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?

a) See AS27001:2006 Introduction (Section 0.2 Process Approach): A process is any activity using resources and managed to enable the transformation of inputs into outputs, and a process approach is 'the application of a system of processes within an organization, together with the identification and interactions of these processes, and their management'.

b) Applicable to all organizations, regardless of type, size and nature.

c) To claim conformity with AS27001:2006, need to comply with clauses 4, 5, 6, 7 and 8.

d) Plan - Do - Check - Act model outlined on page v of AS 27001.

1. Plan (establish the ISMS): Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation's overall policies and objectives

2. Do (implement and operate the ISMS). Implement and operate the security policy, controls, processes and procedures

3. Check (monitor and review the ISMS). Assess and where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

4. Act (maintain and improve the ISMS). Take corrective and preventive actions based on the results of the management review to achieve continual improvement of the ISMS.

e) Management should demonstrate commitment to information security through establishing an ISMS policy, ensuring ISMS objectives and plans are established, establishing roles and responsibilities for info sec, communicating importance of info sec to organisation, providing sufficient resources for ISMS, deciding risk criteria, ensuring ISMS is audited and management reviews the ISMS.

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?

a) See Section 5.1, AS27002:2006. To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

b) Section 5.1.1: The policy document should be published and communicated to all employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader...

c) Section 5.1.1: 'Management should set a clear policy direction' and Section 5.1.2: 'Policy should have an owner who has approved management responsibility for development, review and evaluation of the security policy.'

d) Section 5.2: The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

e) The Information Security policy for QUT is in the MOPP: F/1.2
http://www.mopp.qut.edu.au/F/F_01_02.jsp

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?

a) AS27001 is the specification for information security management systems, a model for setting up and managing an ISMS. AS27002 is the code of practice for information security management. So AS27002 is the stuff you want to do, AS27001 tells you how to go about the process efficiently.

b) Organisations can only be certified against AS27001. They can not be certified against AS27002, because it is a code of practice, not a system specification. Different organisations will make different choices from the clauses in 27002, but they must all follow the process model outlined in 27001, if they want to be compliant.

c) Provides assurance that the organisations take information security seriously enough to commit to a management process, and the

certification means the auditors have checked that they do follow the process.

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?

a) Annualised Loss Expectancy (ALE) in $ for each of the three threats is:

a. ALE(T1: Unauth. access) = $100,000 x 0.02 = $2,000

b. ALE(T2: Unauth. use of comp. fac) = $10,000 x 0.3 = $3,000

c. ALE(T3: Data corruption) = $50,000 x 0.05 = $2,500

b) The spending should be less per year than the ALE, for each of the threats. Although there may be some controls which reduce the risk for multiple threats, so the amounts to be spent could be collected. But spending, say, ten thousand dollars in total to address these three risks may be unjustified, given the tabulated data.

c) Look through AS27002:2006 for possible controls that may be appropriate for ABC.

d) We don't know what ABC already have in place, but this is an opportunity to flick through 27002:2006 and look for low budget items.

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.

a) Malware installed on POS, entry to Target system via subcontractor system.
b) Customer data, including credit card details for 70 million Target instore shoppers.
c) The attackers chose the busiest shopping period, right before Christmas.
d) Yes, they had a malware detection tool that flagged the malware designed to move the data out of Target's systems being uploaded.
e) **Clause 13 deals with information security incident management. It's all relevant to the Target case. Reporting information security events and weaknesses, and managing incidents and improvements.**

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).

a) The study is based on responses from 329 organisations.

b) The average number of laptops

- **a. Each organisation had: 11,174**
- **b. Each organisation lost or had stolen: 263**
- **c. Each organisation recovered: 12**

c) The cost of lost laptop in a 2009 study was $49,246 (Minimum US$1,213 and maximum US$975,527) based on costs associated with:

- **Replacement of device (and software)**
- **Detection of loss (employee time spent trying to recover laptop and reporting incident)**
- **Forensic investigation (by IT employees)**
- **Data breach cost (based on previous cost estimate of $202 per record lost)**
- **Lost intellectual property (or other business information that was not encrypted, multiplied by the probability that it could be discovered and used by competitor)**
- **Lost productivity (based on 2.5 times employee's hourly rate of pay)**
- **Legal, consulting and regulatory expenses**

d) Greatest cause of laptop theft: travel (See page 7 of report).

e) Proportion of lost or stolen laptops with confidential data: (86,455 – 46,686)/86,455 approx 46%.

f) Lost laptop –

- **a. not encrypted: $56,165**
- **b. encrypted: $37,443**
- **c. Difference: $18772.**

g) Consider implementing a program to encrypt laptop contents, if it costs less than $18,772 per laptop (Check out some vendor literature – it doesn't cost anywhere near this amount!)