1

M005

Qualitative Risk assessment & the eTricity Case

1. INF30020 announcements and reminders
2. Groups shaping up and in place by week 6. Group assignment available during semester break
3. This week's class is designed to continue your focus on qualitative risk assessment and individual assignment work.
4. In the activity you will continue to work with your assignment case study to consider, apply and evaluate
   - The connection between theory and practice in risk assessment
   - Best approaches to the description of likelihood and impact
   - ***Based on a consideration of Cloud AND Mobile risks in the eTricity case***

2

Summary, schedule and assessment

Slide 3

Week	Week Beginning	Weekly Teaching and Learning	Assessment and Learning activities
1	01 August	Introduction and Overview: IS risk and security	Class activity & reading (TBA)
2	08 August	Information Security & risks I	Class activity & reading (TBA); Submit CLA #1, Friday 12 August
3	15 August	Information Security & risks II	Class activity & reading (TBA)
4	22 August	Identifying Information Assets & evaluating	Class activity & reading (TBA); Submit CLA
5	29 August	Mitigation, treatment & control I	Class activity & reading (TBA)
6	05 September	Mitigation, treatment & control II	Class activity & reading (TBA); Submit Online Quiz #1, Friday 09 September
		Mid Semester Break – 12 September to 18 September. ISRS Report Part A, due Friday 16 September.	
7	19 September	Information Security & Information Governance	Group Warm-up (TBA); Submit in class, Wednesday 21 September
8	26 September	Business Continuity Management	Class activity & reading (TBA);
9	03 October	Contingency Planning	Class activity & reading (TBA); Submit CLA #3, Friday 07 October
10	10 October	Cybersecurity and Business Continuity Management	Class activity & reading (TBA);
11	17 October	Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring	Class activity & reading (TBA); Submit Report Part B, Friday 21 October
12	24 October	Information Security ethics & compliance and pre-quiz revision	Class activity & reading (TBA); Submit Online Quiz #2, Friday 28 October

Classes

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- M001 completed, M002 completed, M003 completed, M004 underway

Assessments

- CLA#1 , submitted and returned marking in process, CLA#2 submitted
- Individual assignment in progress
- Group expected release dates at end of week 6
- 2 Class quizzes, quiz 1 next week

Groups

Group connections, have commenced

- preliminary formation will be reviewed in this week's face to face classes
- group registration will take place in weeks 6 face to face class

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

Student Check in survey

Slide 4

The one thing..	25% responded
1. Introduction to the Standards (x1)	OK, will aim to do so for S1, 2023
2. Lectures online earlier (x1)	
3. [Improve] description of readings (x1)	
4. Clearer explanations of assignments (x1)	
5. All good, continue to develop (x13 plus)	Why is it a core unit? Its core IS & InfoSec curriculum. Industry requests same

Above faculty average & means

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

Takes place in Week 6

Slide 5

Challenge Quiz No.1 (Online Quiz)

will take place during Week 6, from 9:30am Thurs 07 – 9:00pm Friday 08 April

Where's the Challenge? **15 questions in 25 minutes**

Completion of the quiz during date and time range is a unit requirement,

The quiz will cover topics from Weeks 1-5, with a focus on contents covered in lectures and Face to Face classes

All questions will be multi-choice &/or selection based

There are no other continuous learning activities during week 6, all classes as normal

Further details, see the instruction page in CANVAS modules

5

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

5

Readings in support of Qualitative Risk Assessment

Unit texts:

1. Whitman, Michael E. annd Mattord, Herbert J. Chapter 6 Risk Management, Risk Assessment. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, 2018.

1. Gibson, Darril, Chapter 5 Defining Risk Assessment Approaches. *Managing Risk in Information Systems*. 2015.

x

Suggestions from additional reading list

1. Schmittling, R. & Munns, A. Performing a Security Risk Assessment, ISACA Journal, 2010, Volume 1, https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx

2. Thomas R. Peltier (2004) Risk Analysis and Risk Management, Information Systems Security, 13:4, 44-56,Swinburne Library link: http://ezproxy.lib.swin.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=14451647&site=ehost-live&scope=site (Links to an external site.)Links to an external site.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

6

Case Report Part A: is all about identifying & assessing

Take a step wise approach & use these steps to model your assignment:

You are an external auditor hired by eTricity to complete and report on an overall security risk assessment for the organisation:

- ✓ Propose a target risk appetite and risk tolerance level for the eTricity (week 3- 4),
- ✓ Identify the key roles and responsibilities of individuals and departments within the organization as they pertain to risk assessment (week 3- 4),
- ✓ Carefully audit the case evidence, undertake an inventory and identify information assets (***table or list of assets***) that includes both, eTricitys most significant business information assets and the information systems that must be accounted for in any approach to risk management (week 2- 4),
- ✓ Identify risks: provide an analysis of the threats and vulnerabilities that pose the greatest risks to eTricity most important information assets (information and systems) (weeks 2-4)
- ✓ Present a likelihood and impact analyses for the most significant risks you have identified, and in doing so, (weeks 2-5)
- ✓ Prioritise the most significant risks for eTricity and provides details in a risk assessment table &/or statements. (weeks 2-5)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

7

A risk assessment results in a report that management will use to plan how to control for risks to information assets.

It starts by identifying where and what the information risks are,

- It has an Executive summary followed by an,
- Introduction that is is context dependent: business strategic context, value creating activities, appetite, tolerance & threshold; who is responsible &/or who should be.
- The body of the report is about: ***identifying and reporting assets, their vulnerabilities and potential threats.***
  - It needs to describe (and evaluate) strengths of approach taken; details on the information systems and information assets,
  - It requires analysis: how severe is the current level of risk? (e.g. costs, likelihoods and impacts associated with risks,

    It needs to describe (and evaluate) the qualitative risk assessment approach taken.
  - It includes your evaluation (i.e. Is the current level of risk acceptable?) Needs qualitative risk assessment results (tables & or diagrams)
- It ends with a conclusion &/or recommendations. You need to prioritize the risks and present recommendations so that your assignment team will (eventually) know what we want to treat, mitigate for. **No** recommendations on controls at this stage
- ***Your format should make it easy for management to understand the highest risks based on your assessment***

8

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

8

Activity A: Peltier & risk assessment

Reading: Peltier, Thomas R., (2004) Risk Analysis and Risk Management, Information Systems Security, 13:4, 44-56,

1. What are the three deliverables of risk analysis as described by Thomas Peltier?
2. What are the 6 steps associated with these?
3. What 'fit' do you see between the work you are undertaking in your risk assessment fort eTricity and deliverables described by Peltier?

9

Activity B: Qualitative risk assessment

With respect to your work on the eTricity case:

What qualitive risk assessment approach are you settling on and why?

Choose the closest corresponding option. When answering briefly explain what you consider to be the main strengths and weaknesses in the option your considering (consider at least 1 of each – a strength and a weakness)

a) Using a simple descriptive ranking (e.g. low, medium & high)
b) Using a more nuanced descriptive ranking (what categories did you decide on?)
c) Using an ordinal rating system (what ratings did you decide
d) Using a combination of rating and ranking (value & range), why?

10

Activity C. Cloud & Mobile risks at eTricity

Make a quick decision to focus on *1 or the other*: *either,* ***Cloud*** or ***Mobile*** computing considerations in the eTricity Case and address the following tasks:

1. Identify either two significant Cloud OR or two significant Mobile 'risks' present in the case study.
   i. -------, why?
   ii. -------, why?

2. Prepare an explanation for the class on why have you decided on these two? Have you consider OCTAVE in your decision making?

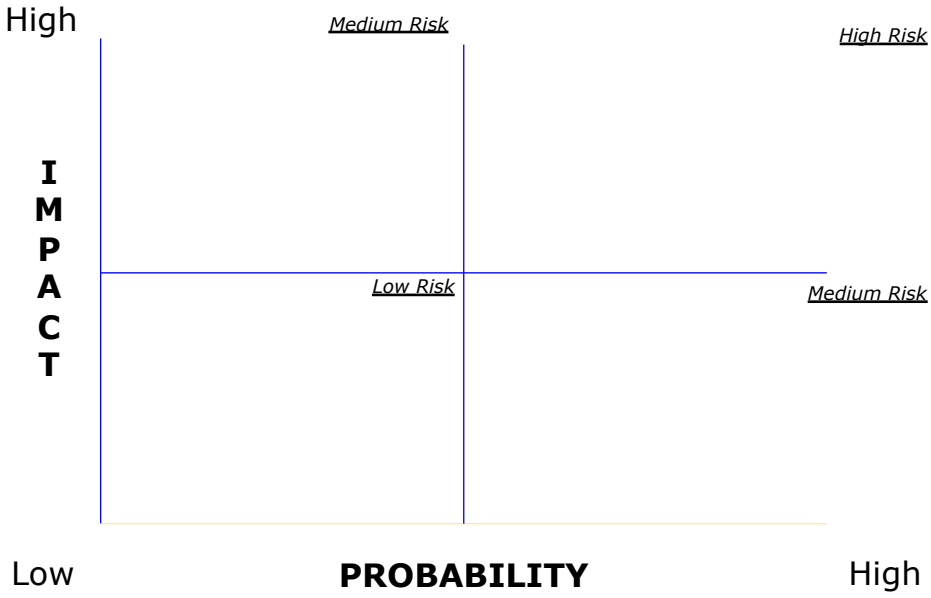
Activity D. Describing likelihood and impact

Continuing to work with the same three significant ***Cloud*** or ***Mobile*** 'risks':

1. Complete the Impact & Probability matrix provided for with today's handout by locating your 3 risks on the matrix
2. Do you think this matrix is a suitable descriptive vehicle for describing the the likelihood and impact of risk at eTricity, Why or why not?

Also see Q's 3 & 4

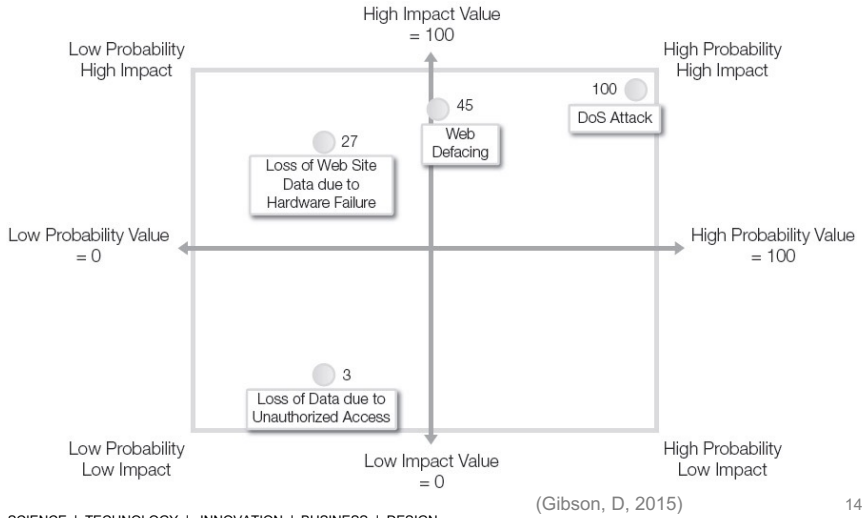
Impact versus probability chart



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

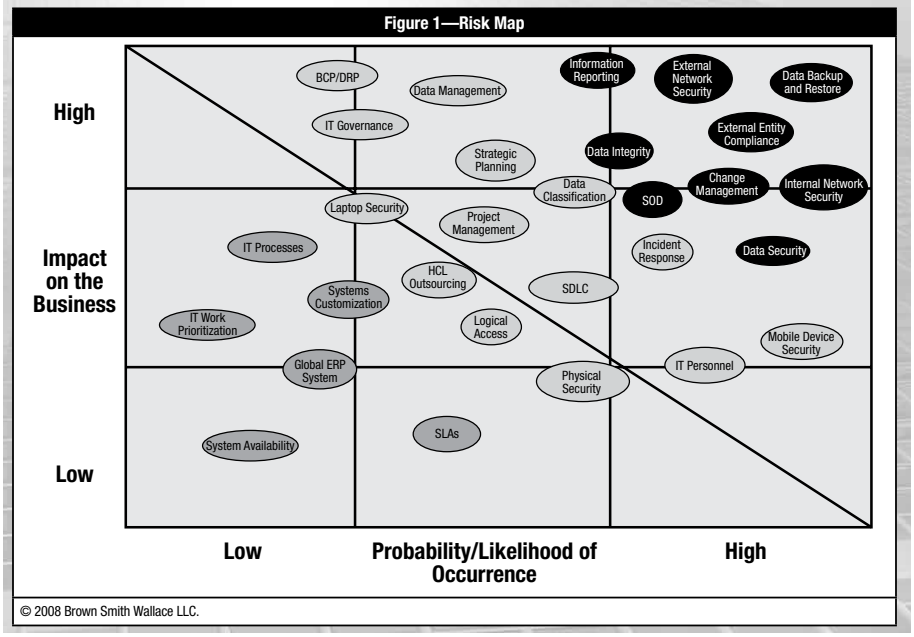
13

CATEGORY	PROBABILITY	IMPACT	RISK LEVEL (1 to 100)
DoS attack	100 percent	100	100 (1.0 × 100)
Web defacing	50 percent	90	45 (0.5 × 90)
Loss of data from	30 percent	10	3 (0.3 × 10)
Loss of Web site data due to hardware failure	30 percent	90	27 (0.3 × 90)



(Gibson, D, 2015)

14



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

15

Activity E. Describing likelihood and impact

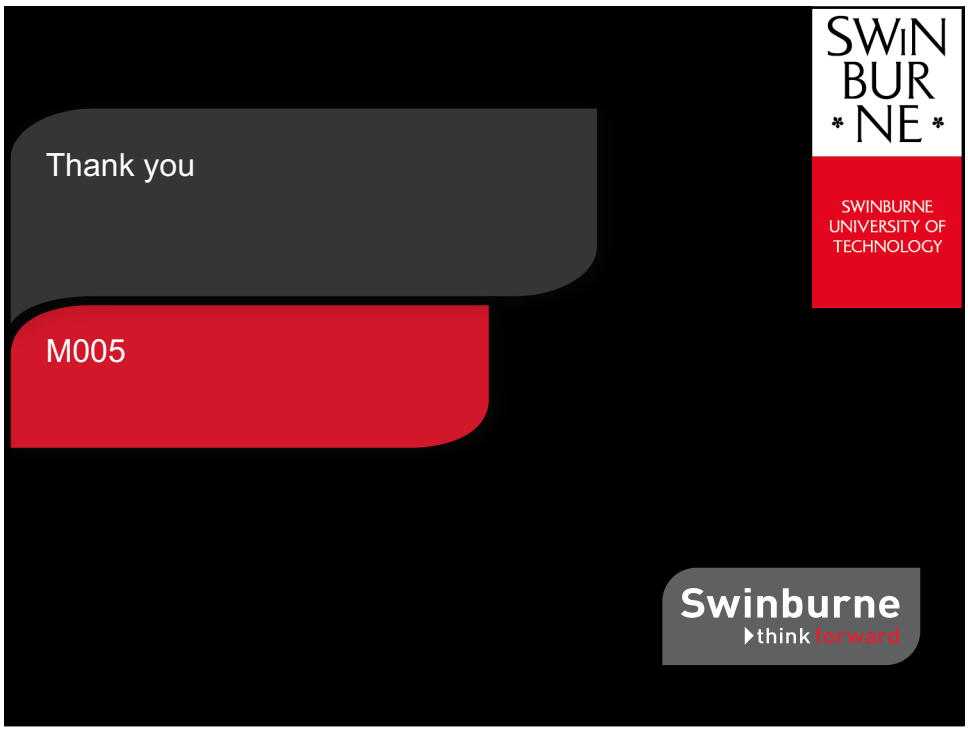
Continuing to work with the same three significant ***Cloud*** or ***Mobile*** 'risks':

After answering Q1 & 2

3. How can you improve on this matrix? Take a look at the examples provided on the subsequent slide from Darril Gibson's, do you think it improves on the simple matrix, why?
4. Answer this question by preparing a better and enhanced response in your own assignment for *likelihood* and *impact, prioritisation,* Before doing so you might like to consider the TVA worksheet on page 341 of Whitman (Table 6-8) AND the risk map represented by Ron Schmittling,

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

16


Thank you
M005
SWINBURNE
UNIVERSITY OF
TECHNOLOGY
Swinburne
think forward

17