1

Summary, schedule and assessment

Slide 2

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	Assessing security and establishing Internal Control	Class activity & reading (TBA); Submit CLA #2, Friday 26 August
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

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

Classes

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- Week 1, M001 completed, week 2 M002 available

Assessments

- CLA#1 , due Friday 12th August, submitted , marking in process
- Individual assignment released
- Group expected release dates at end of week 6
- 2 Class quizzes

News

- Guest presentations
  - Program to be confirmed
- ISACA student group
- *All parts of unit of study are relevant to you learning and assessment*

2

This week's learning plan

Slide 3

1. Risk & Risk management (reminder to week 1 Week 2)
2. Risk assessment
   a) Risk management process
   b) Risk appetite & tolerance
   c) Risk identification
   d) Analyse risks
3. Information Security & Internal Control (week 4)

3

Keep reading, keep listening, keep active

Slide 4

Required & recommended readings

1. Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning,

   Chapter 6 & 7 highly recommended for your major assignment Part A & Part B assignment

2. Support reading Gibson: Chapters 4-6

3. Moeller, Robert R (2007) COSO enterprise risk management understanding the new integrated ERM framework (library ebook) chapter 3

4

The role of standards

Slide 5

- Issued by a standards body, e.g. Standards Australia or ISO.
  - the outcome of a defined industry need.
  - **developed by industry.**
  - **agreed to by industry.**
- Accepted specifications or codes for practice ***assisting to define materials, methods, processes and practices*** used for industry or by a professional body. Support policy development and decision making,
- Basis for determining consistent and acceptable minimum levels of quality, performance, safety and reliability. Suppport business improvement, benchmarking practice,
- Familiar examples include Design Standards (or Codes) e.g, Australian Design Rules (car emissions) product safety; here standards providing guidance on safety for health, life and property matters,
- There are also competency standards – setting benchmarks for qualifications in professions, e.g. ISACA certifications,
- Enables compliance and provides evidence Issued by a regulatory authority or prescribed under a regulatory requirement e.g. National Privacy Principles and the Privacy Act ; ADR, Motor Vehicle Standards Act 1989

5

Preparing for assignment

Slide 6

Familiarise yourself with Required readings

1. ***AS ISO 31000:2018* : Risk management – Guidelines**

   http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/806031 (Links to an external site.)

2. ***AS/NZS ISO/IEC 27005:2012* : Information technology - Security techniques - Information security risk management**

   http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/862854 (Links to an external site.)

Recommendation: start with the Executive summaries, familiarise yourself with general content researching more detail towards assignments

Access details via Library: TechStreet Standards dB

Recommended introductory reading for week 3, focus on Risk assessment

Whitman Chapter 6 & 7

6

Preparing for assignment 1

Slide 7

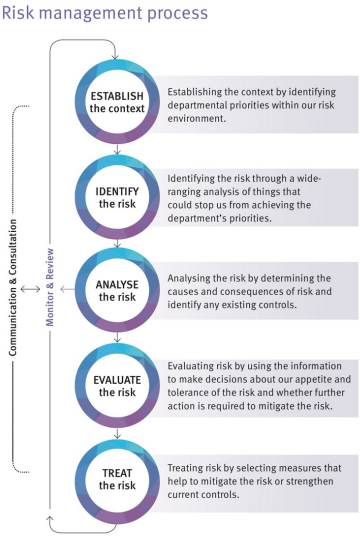
Familiarise yourself with Required readings

Access details will be provided in CANVAS

1. ***AS ISO 31000:2018* : Risk management – Guidelines**
   Start with its first 16 pages

2. ***AS/NZS ISO/IEC 27005:2012* : Information technology - Security techniques - Information security risk management**
   Start with pages 1-9

familiarise yourself with general content
researching more detail towards assignments



7

Individual assignment tasks

Slide 8

Its all about identifying information assets and assessing and prioritising risks so that information is secure

You are to take on the role of an external auditor who has been hired by the eTricity to undertake an overall (general) information risk assessment and prepare a report with the aim of securing information assets for the organisation:

1. **Explain your approach to Information Security risk management and risk assessment** to eTricity; i.e. let your clients know what risk management for InfoSec is is and how you will approach it,
2. **Assess and describe, eTricity's strategic environment**, their value creating activities and current risk posture; propose a target risk appetite and risk tolerance level in report,
3. **Identify and table the key roles and responsibilities of individuals and** departments within the organisation as they pertain to the management of information assets and assess associated information risks,
4. Audit the case study to **identify and prepare a full inventory** (descriptive list) of information assets that includes eTricity's most significant, information resources, for sound information security management and risk management. Include your list as an appendix item,
5. Include an ATV table in your report identify risks (threats and vulnerabilities) for the **top 7 information assets identified**: provide a supporting explanation for your analysis of the threats and vulnerabilities for eTricity's most important information assets (both information and information systems/processes),
6. **Present a likelihood and impact analysis** for the **seven (7)** most significant information assets/risks
7. **Evaluate and prioritise the most significant associated information risks** for eTricity to manage in your assessed order in your risk assessment table,
8. Your report should be **supported with well-described, images and tables.**

8

This week's learning plan

Slide 9

Focus on your familiarity with the following concepts

Risk assessment

a) Risk appetite & tolerance

b) Risk identification

c) Analyse risks

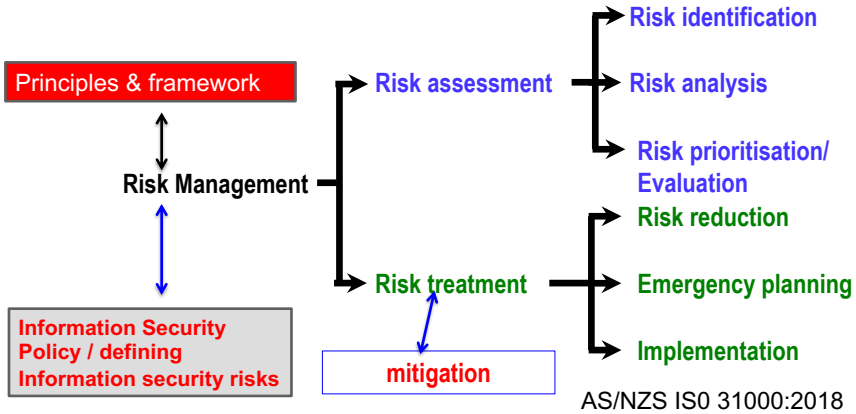
Within risk assessment process

9

Risk assessment, mitigation & treatment

Slide 10

After the risk management (RM) process team has identified, analysed, and evaluated the level of risk currently inherent in its information assets (i.e. an information risk assessment), it must then treat the risk that is deemed unacceptable when it exceeds its risk appetite. Treating risk begins with an understanding of what risk treatment strategies are and how to formulate them

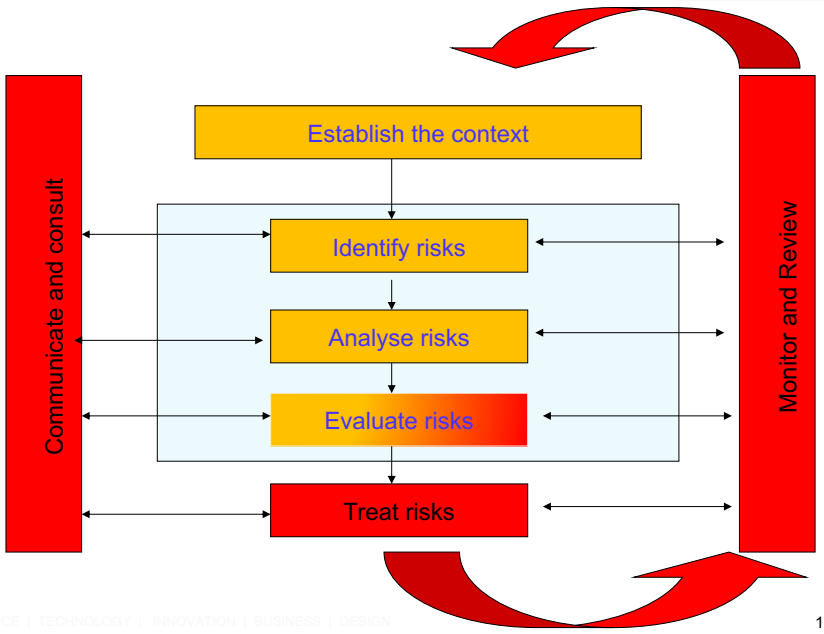


AS/NZS IS0 31000:2018

10

Risk assessment ISO 31000: 2018

Slide 11

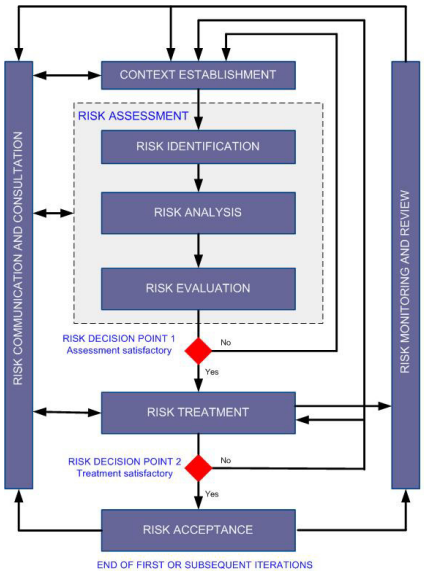


11

11

Risk assessment, ISO 27005: 2012

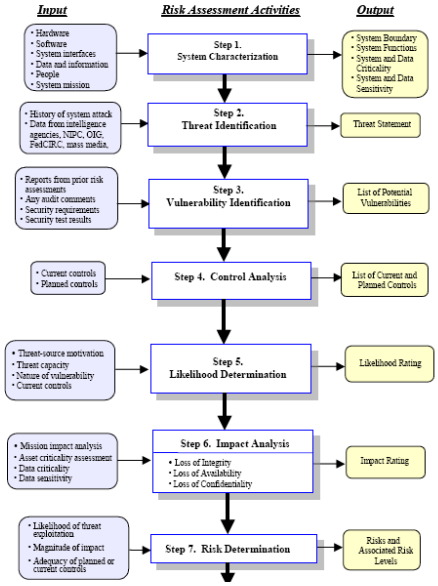
Slide 12



12

Risk assessment

Slide 13



NIST SP800-30 – Guide for Conducting Risk Assessments

practical guidance necessary for assessing and mitigating risks identified within IT systems

13

Risk assessment

Slide 14

Risk assessment can be read directly as your Assignment*: Part A*

- Identify: where and what are the risks are to the organisation's information resources?
  - Identify assets
  - Identify vulnerabilities
  - Identify threats
- Analyse : how severe is the current level of risk to information assets ?
  - e.g. costs and impacts associated with risks / not managing the risks
- Evaluate: Is the current level of risk acceptable
  - Prioritise the risks we want to treat
- Present recommendations

14

Risk assessment

Slide 15

Risk assessment reporting requirements

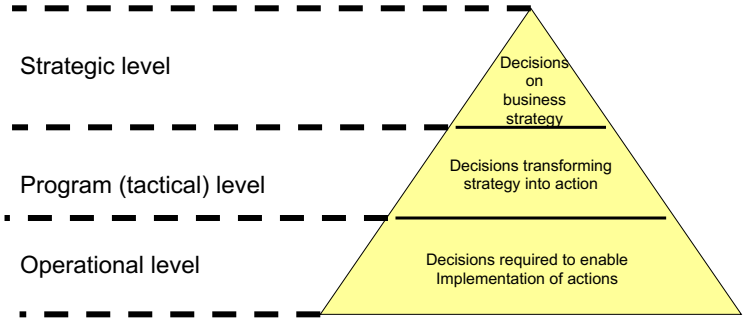
- Report should include:
  - Context setting (overview, risk appetite & tolerance)
  - Findings (in terms of an inventory of assets, vulnerabilities & threats)
  - Risks statements: Risk are often summarised in risk statements, i.e. you can use a risk statements to communicate a risk – likelihood and consequences - and the resulting impacts, could be done as an ATV table

Risk assessment

Slide 16

What is risk assessment

Risk assessment is the identification, analysis and priortisation of risks to support the achievement of business objectives. It is the process of applying risk management to the specific risks an organisation faces. It forms a basis for determining how risks should be managed in orgsanisational contexts.



[Source: IT Governance Institute. 2005 Information risks: Whose business are they? Page 12]

Risk assessment

Slide 17

Establishing the context our starting point is COSO's ERM

Enterprise Risk Management is *a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across an enterprise, designed to identify potential events that may effect an entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding achievement of entity objectives*

COSO, ERM framework 2004

- A strategic understanding of an organisations information resources
- Establishing a philosophy that recognises expected and unexpected events and emphasising control of effect
- Governance of risk, identifying, assessment, acceptance, communication & treatment

17

Risk assessment

Slide 18

What it is: Strategic understanding of information value

- The strategic objectives, how, why, what information is most critical. Value of other information assets
- A clear idea of information needs and how staff use information , the value creating activities of the organisation
- Having this should
  - Support decision making
  - Focus resources efficiently and effectively
  - Legal requirements, innovation, production
  - Identifying the information assets first, allows us to assess information risks & plan for business continuity

18

Risk assessment

Swinburne

Who is responsible, for what information? *What questions can you ask of your case?*

Role	Responsibility
BOD	▪Be aware about IT risk exposures and their containment ▪Evaluate the effectiveness of management's monitoring of IT risks
IT strategy committee	▪ Provide high-level direction for sourcing and use of IT resources, eg. strategic alliances ▪Oversee the aggregate funding of IT at the enterprise level
CEO	▪ Adopt a risk, control and governance framework ▪Embed responsibilities for risk management in the organisation ▪Monitor IT risk and accept residual IT risks
Business executives	▪ Provide business impact assessments to the enterprise risk management process
CIO	▪ Assess risks, mitigate efficiently and make risks transparent to the stakeholders ▪Implement an IT control framework ▪Ensure that roles critical for managing IT risks are appropriately defined and staffed.
[Source: IT Governance Institute. 2005 Information risks: Whose business are they? Page 14]	

19

Risk assessment: in context

*(a) **Risk appetite*** and risk tolerance

- Establishes (sets the scene for) the Enterprise's risk culture
  - *The critical point is that risk strategy (and through that security) is aligned to the business objectives of the organisation, i.e. its value creating activities and its future directions*
- Risk appetite is a strategic conversation, its a high level view (a formal statement) of how much risk management (and the board) is willing to accept
- Risk appetite is often expressed in terms of tolerance; both in quantitative and qualitative terms (e.g. earnings at risk versus reputation risk) and the considered risk tolerance (range of acceptable variation)

20

Risk assessment

Slide 21

(a) Risk appetite and ***risk tolerance***

- Risk appetite the high level – strategic - conversation focussed on driving business direction with a suitable risk profile
- Risk tolerance is a – tactical – conversation, linking risk appetite to metrics and measures that can be monitored
  - e.g. articulating a strategic preparedness to take risk by extending business into the BRIC markets (Brazil, Russia, India, China) expresses *an appetite* and sets the organisational tone
  - Identifying the specific market to enter (a measure) and the acceptable level of variation around performance targets for those markets (metrics) expresses the tolerance
  - E.g. Amazon typically allows 7 years to establish a market share its happy with

21

A review of the process

Slide 22

- **Identify**
  - Business strategy, objectives, (…value, appetite & tolerance)
  - Assets
  - Vulnerabilities
  - Threats
- **Analyse**
  - Likelihood and consequences
  - Impact
  - Existing controls
- **Evaluate**
  - cost of exposure versus cost of protection
  - **Priortise risks** (for treatment)

22

Risk assessment

Slide 23

(b) Risk identification

- Processes for identifying the risks and opportunities that could impact on an organisation
- At the strategic, tactical and operational levels, considering how an organisation best achieves its outcomes and *ensures the protection of its assets by* examining all ***sources*** of risk to **assets**
- **It is an IT/IS audit (inventory and analysis) approach that focuses on the effects of information assets being put at risk**

23

Risk identification

Slide 24

Information assets and information audits

- In IT/IS security risk assessment takes on many names and can vary greatly in terms of method, rigor and scope, but the core goal remains the same: identify and quantify the risks to the organization's information assets.
- The assessment approach analyses the relationships among assets, threats, vulnerabilities and other elements
- What constitutes an information asset will be specific to the organisation (and this is why the approach or methodology becomes more important). Assets might include, *Network architecture and infrastructure, customer records, intellectual property, other corporate records essential for the operation of the business, web services essential for the operation of the business, knowledge of the organisation's business processes*
- ***You get the picture! it is all about 'what is essential to continue business operations'***

24

Risk identification

Slide 25

Information assets and information audits

- Systematic examination of information assets/resources, their use and flow (e.g. dissemination information internal and external, information available to the public)
- How? Document analysis, verification by people (interviews, surveys. Focus groups)
- How? Undertaking an inventory of existing information and systems (digital work environments, databases, electronic and paper information exchange, network architecture, applications)
- How? Isolate the most significant information assets and systems (e.g. plans, financial recrods, email, social media)
- **Indicate what is important to protect (i.e. control)**

25

Risk identification

Slide 26

Risk, threats & exposures and vulnerabilities

- Threat

  Potential cause of an unwanted incident*, which may result in harm to (an asset) a system or organisation* ISO/IEC 27000:2009

  The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability NIST SP 800-30

- Vulnerability

  Weakness of an asset or control that can be exploited by a threat ISO/IEC 27000:2009

  A flaw or weakness in system security procedures, design, implementation, or internal controls NIST SP 800-30

  judgement error, unexpected transactions or events, collusion, management override, conflicting signals

26

Risk identification

Slide 27

Assets, threats & vulnerabilities

1. Identify assets,
2. Examples: **ABS Census** and at risk if threatened or exposed are,

   Personal data of Australian citizens and aggregate data about Australian citizens, **data timeliness**, **IT Infrastructure** (if **interrupted** e.g. by DDOS attach or load), Data acquisition, **Data availability**, Data confidentiality, Data Integrity (if breached)

2. Identify and assess ***Vulnerabilities*** to ***threats/exposures***

   Examples: ***communication and receipt of information*** via malicious ***DDOS attack or ill-prepared server provision for load***

3. Determine acceptable risk levels, assess the probabilities of likelihood and impact of vulnerabilities being exploited

   Example: (i) **Interruption to communication** would have an extremely negative impact and pundits at the time were saying was likely; however in this case it appears as though the risk was not assessed highly enough

27

2(c). Analyse risks to information assets

Slide 28

Likelihood and consequences

1. Likelihood
   - The probability of a risk eventuating

2. Consequence
   - The impact of an adverse change to the level of business objectives achieved

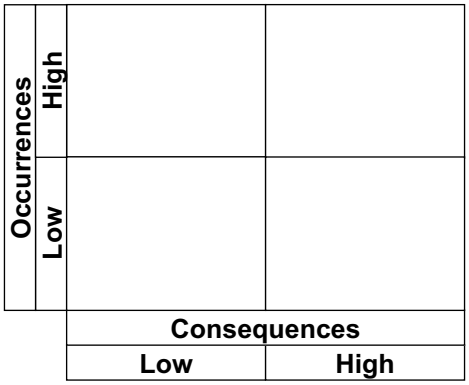
3. Existing controls
   - Safeguards and countermeasures in place to manage risk

28

2(c). Analyse risks

Slide 29

Jacobson's window



Robert Jacobson, 1997

Isolates four classes of risk -- low-low, high-low, low- high, and high-high. These four are easily broken down into either inconsequential or significant risk classes. E.g with a focus on 3

29

2(c). Analyse risks

Slide 30

Impact versus probability

IMPACT		
High	*Medium Risk e.g. fire damage* **Share**	*High Risk e.g. DDOS attack* **Control (reduce, mitigate, avoid)**
	Low Risk Staff availability **Accept (monitor)**	*Medium Risk e.g. spam email* **Control (Reduce)**
Low	**PROBABILITY**	High

30

2(c). Analyse risks

Slide 31

Categorisation of risk exposure

- Options available:
  - Accept = monitor
  - Avoid = eliminate *(get out of situation)*
  - Reduce = institute controls
  - Share = partner with someone *(e.g. insurance)*
- Residual risk *(unmitigated risk – e.g. shrinkage)*

Residual risk = inherent risk - impact of risk controls

31

2(c). Analyse risks

Slide 32

Example: Call centre risk assessment

IMPACT		
High	*Medium Risk - share* • Fraud • Credit risk / or other information risk	*High Risk- avoid* • Loss of phones • Loss of computers • Customer has a long wait • Customer can't get through • Customer can't get answers
Low	*Low Risk- monitor* • Lost transactions • Employee morale	*Medium Risk - reduce* • Entry errors • Equipment obsolescence • Repeat calls for same problem
	PROBABILITY	High

32

2(c). Prioritisation of risks

Slide 33

33

2(c). Prioritisation of risks

Slide 34

Determining acceptable risk levels

- Evaluating risks on the basis of the *likelihood* of and *consequences* provides two factors that can be used to prioritise risk management
- Specific risks can be ranked on the basis of the evaluation
- Using ranking and rating systems the order for addressing the risks can be determined

34

2(c). Analyse risks

Slide 35

Key elements of likelihood analysis

- Estimations the probability of a threat(s) occuring
  - Probability of Occurrence (High, Medium, Low)
  - Category Ranking – nominal or numeric, (e.g. 7-10 = High,4-6 = Medium, 1-3 = Low)
  - Ordinal Ranking (a weighting, e.g. a numeric weighted impact factor)
  - Relative Likelihood of Occurrence (risk in doing a, compared to b)

(Applying COSO's Enterprise Risk Management Integrated Framework: http://www.coso.org/erm-integratedframework.htm)

35

2(c). Analyse risks

Slide 36

Key elements of impact analysis

- Assess the degree of harm or loss that can occur as a result of exploitation of vulnerability
  - a.k.a impact assessment, consequence analysis, consequence assessment
  - Rate or rank
  - Calculating the cost of exposure
  - Both direct and indirect business impacts

    e.g. immediate financial impact (cost) of losing an asset

    e.g. cost of advertising to counteract negative publicity

36

Determining acceptable risk levels

Slide 37

Figure 6-10 Clearwater Compliance IRM risk rating matrix

Source: Clearwater Compliance IRM.

Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, Chapter 6

37

Determining acceptable risk levels

Slide 38

Table 6-12 Risk Rating Worksheet

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5

Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, Chapter 6

38

Determining acceptable risk levels

Slide 39

Figure 6-12 Clearwater Compliance IRM risk threshold

Source: Clearwater Compliance IRM.

Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, Chapter 6

39

Terms & processes to follow up on

Risk assessment, Risk appetite, Risk identification, Analyse risks /evaluate risks

SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne think forward

40