Swinburne University of Technology Faculty of Business & Law   
INF30020 Information Systems Risk & Security   
Semester 2, 2022   
Report Part A   
Word limit: 2500 words   
Due: Friday 16th September 11:59 p.m. (AEST)   
Please refer to the eTricity 2022 Case Study for this assignment   
You are an Information Systems Security Auditor who has been assigned to eTricity to carry out an   
information risk assessment for the solar energy specialist. Your task is to produce a 2500-word auditors   
report (in business report format). Your report should address the following specified components:   
  
Prepare an information security risk assessment. To do so, you must:   
1. Briefly explain your approach to Information Security risk management and risk assessment to   
eTricity; i.e. in an approximately 100 to 150 word introduction let your clients know what risk   
management for InfoSec is is and how you will approach it,   
2. Clearly and concisely 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. Carefully audit the case study to identify and prepare a full inventory (descriptive list) of   
information assets that includes eTricity’s most significant, physical &/or logical information   
resources, information of value and the information systems/process required 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 (asset)   
risks you have identified, in doing so,   
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.   
In preparing your risk assessment report you are NOT TO extend beyond this brief, i.e. you are not to   
prepare any other components of a risk management plan (mitigating or treating risks). In prioritising   
your risks, you may table all other information assets and risks that you have identified, but do not   
undertake a likelihood and impact analysis or prioritisation of any except your chosen top 7.   
At this stage, do not propose any risk treatment (management solutions or internal controls), that will   
come later in your group assignment   
Following the completion of the risk assessment report part A, eTricity will evaluate the next steps for   
your consultancy. The risk assessment needs to be conducted in accordance with best practice and   
should apply (one, or a hybrid combination of) the leading standards, guidelines or frameworks

pertaining to IS risk and security management. Your report must articulate clearly which   
standards/guidelines it has followed and how they have been used.   
You are to prepare your risk assessment report for eTricity’s Directors and your report should be written   
as a formal business report that is suitable for your audience. Guidelines for business report writing can   
be found at the Faculty of Business and Law, Swinburne subject guide:   
https://www.swinburne.edu.au/current-students/study-support/resources-  
materials/assignment-writing-guides/   
  
In addition to your use of standards and guidelines for the risk assessment report, you should research   
and consult secondary sources in your work and in presenting your report follow standard academic   
referencing procedures for the Harvard Style:   
http://www.swinburne.edu.au/lib/studyhelp/referencing.htm   
The following should be included with your risk assessment report   
• An Executive summary (for a good description of a what comprises a good ES see,   
https://unilearning.uow.edu.au/report/4bi.html)   
• Relevant appendices for the report (should be used as you deem appropriate and will not be   
counted in word limit),   
• A report reference list that applies the Harvard style guide (in text citation is an expectation for   
this report).   
• All reports must be presented in standard 12-point font   
Your report will be submitted online in CANVAS.   
Please note for planning report structure and word limit: The assessment criteria for this report focuses   
on your analysis and explanation of the risk assessment you undertake. While all appendices, tables and   
diagrams used in the report will contribute to your assessment, they do not count towards the word limit   
for the assignment. Your executive summary and reference list will also not count towards the word limit.   
However all diagrams and tables in the report or in the appendix added to the report must be relevant,   
significant and well supported (through written description) in order to count favourably towards your   
assessment. Where devices like the Executive Summary, Appendices; diagrams or tables that have been   
used simply to extend the allowable length of the assignment, they will not be assessed.

-----work with unit books mostly and the ISO 31000 stuff indepth+++ reference them (including the materials released in the f2f classes. So try to bring all of those up as primary info source, alongside etricity case)

Work fed into standards…

Defines risk, asset, etc + systemetic approach to info asset and sec+

Say followed starard’s by doing………(thus did my “due diligence” and assure etrictrity)

Mainly follow it for risk identify, analyse, evaluate--- try to continuously reference it and whitmann for terms and method used

+iso27005 (focus into ict device and software a bit more)

Breakdown catagoies with tables in it saying typical threat and vulnerability examples to different orgs---can verify whther ur vul and theart are correct or not---- also reference it (mainly use it in middle type area)

(near the end or evaluation parts)

+NIST stepwise model--- for scoring or rating system for ranking atv stuff anf risk stuff--- say rating catagories, then later use anothee table to explain the rationale behind the point

Must focus on threat, asset and vulnerability system (USE ATV---maybe NIST might miss some parts of the ATV so beware!)

Keep risk assessment at “higher level” for tolerance framework

(not just google stuff)