Starting page:

Your name, id

Course name, course id

Title of report, etc ---see the format used by those two papers…..

Content list:

Executive summary

Introduction

Strategic Environment, Risk Appetite & Risk Tolerance (merge it with the introduction )

Roles and Responsibilities Identification

Information Assets Identification

Threat, Vulnerability and Risk Identification

Likelihood and Impact of Risks

Prioritization of Identified Risks

Conclusion

References

Executive summary

---Write this after finishing the risk analysis and whilst writing the conclusion part.

---Here you need to say…. What the company is and what it does, when and where it was established, what is their current issue (or you can just generally say that their activities had lead to several problems regarding …. (just note the info assets)).

---Then say that, hence this report has been made in order to analyse and catagorise these issue in order to understand the vulnerability, threat, and risks associated with them. Furthermore, in order to comprehend the true risk, likelihood and impact analysis have also been done on the most significant 7 issues that it had faces with their outcomes noted in ……………..likehood and impact of risk ending and………prioritization of identified risk. After this the report had been concluded by giving some brief general information/ recommendations about the steps it should take in the future, now that the risks have been identified and analysed.

thus, the company has hiered you as an

Introduction

Explain what the company is about and what it does in brief (like company… is solar panel company or smth that focused on…. (directly quote from case study)). Then say what you will do (ie that you will audit their system’s risk management from info sec perspective. This means…… by………..

---what info security (refer to whitmann ch 1 for this)+ risk management + Risk assessment for InfoSec is ---maybe use reference from proviti?

---how to approach risk assessment--- class handouts? (see week 5 f3f lab note for hints on where to find info)--- Say followed starard’s IS31000 by doing………(thus did my “due diligence” and assure etrictrity)

(maybe analyzing their info assets, threats, vulnerabilities and risks in depth and prioritizing them ---make it more informative whilst reducing words too!)

Strategic Environment, Risk Appetite & Risk Tolerance (merge it with the introduction!)

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,

---explain what strategic environment is+++ link it to etricity (value in creating activities and risk posture—current one)

---then exaplin how it leads to Risk appetite and tolerance (---if you cant find link, then just link it to RISK and then say according to ISO…. This can be done by performing risk appetitie and tolerance++what these terms means in brackets++)

Then say that currently case study didn’t provide you with one and thus you have devised the following risk appetite and tolerance to follow

---write risk appetite and tolerance in terms of etricity (take help from slides in week… where we compared the two different versions of risk appetite ++ also see the CLA#2 beginning part to get hint on how to write it++ make it brief and with a slider to show place where risk will be and wouldn’t be accepted)

---maybe ISO31000:2018 ++ proviti may help with this?

Roles and Responsibilities Identification

---for here, say that according to “Peltier” “risk management is an enterprise management responsibility” where each person (and group) have different roles and responsibility… then say that to make it easier to understand this, you have given a table:

|  |  |
| --- | --- |
| Role | Responsibility |
|  |  |

--take help from CLA#2 for this---also go through etricity ones more just in case to ensure you didn’t miss anyone’s name—for responsibility, must include all their responsibilities, not just ones noted in cla#2!! (ensure focus is on info asset!)

Information Assets Identification

---explain what info asset is+++ (reference to ISO27000 pg 14 ---in pdf scrolling page search type 22) ++ say its importance to business ++also use another better reference for info asset---like maybe whitmann?? and thus explain why is it continuously under attack. Then say that here you made a table to better understand the info assets present in the case study:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Asset Name | Asset Type (hardware, software/data, people) | Asset Storage | Asset details | “Value of Asset”  Importance to company (use a chart of low, medium, high)---using whitmann I think-----  Then include another table below to explain what the low medium and high means |
|  |  |  |  |  |

---like say system critical or not…..

|  |  |
| --- | --- |
| Value of Asset | Meaning of the Value ---like in terms of org success, org profit, expensive to replace/ protect, loss that will case greatest liabioity/ embarrassment---whitmann ch 262-262 for the points |
|  |  |
|  |  |
|  |  |

Threat, Vulnerability and Risk Identification

+++ explain what threat, vulnerability means and how they link to risk….Then say that you are going to create an OCTAVE table where it explains each vulnerability and threat in details)….

---following words of Whitmann (pg 309---333 in the scroll pdf pg no.)……. for the top 7 issues/ info assets at risk..etc asit allows orgs to…. Iterate what whitmann said in own words … (

to make it easier to understand and help focus on important/critical points (only make 7!! And only say about the most significant ones)---

(hint—write the asset first then say its related vulnerability and thus the outcome threat)

+++say what operation critical means and give either a general reason on why these are operation critical (like say you have taken these as “operation critical” as they fulfill points like…..) or explain each point---(maybe give reference to a soruce in google or go through lect note from week 13 or do both)

+++ USE NIST (scroll 69-75 for different threat example and importance) ++ (USE)

|  |  |  |  |
| --- | --- | --- | --- |
| Operation critical (add a note saying that all of these are operationally critical so just gave numbers to give their ranking relative to one another) | Threat (name the threats---and then explain what is ) | Asset | Vulnerability (name the vulnerability---and then explain what is ) |
|  |  |  |  |

Note: ……saying that all of these are operationally critical so just gave numbers to give their ranking relative to one another+++ say that will use these numbers to further refer to these records in the table

Likelihood and Impact of Risks---NIST?

----say smth like….although knowing about the threat and vulnerability of a threat does help us understand that a risk exists, it is not enough for us to understand how severe it actually is> instead, following the words from NISt is it better to use…..and …. as risk is….. +++((reference to NIST) pg-6 (scroll 15 ) for link between likelihood and impact with risk)

---Explain what likelihood and impact of risk is ….+++ NIST pg 10,11 (scroll 19,20) for defn of likelihood and impact.

----then say smth like, thus I am expanding upon the previous table to include the likelihood and impact of each risk

(Note: only including the operational critical number to link the table instead of repeating the threat, asset and vulnerability once more as:

the critical number is currently uniquely identifying them,

it makes the information in the table more easier to read and understand)

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Critical number | Likelihood score (1-100) | Impact score (1-100) | RISK Score (Likelihood \*Impact)  (1-10,000) |
|  |  |  |  |

Furthermore, in order to better understand what the scores in both likelihood and impact mean, I have used the following tables from….. (NIST Likelihood table scroll to 82 and merge the info in the 3 tables) and…. (NIST Impact table scroll to 85)

(table explaining what numbers means for likelihood)

(note: here I had merged the likelihood tables for the threats as currently I am noting the chance of all the types of threats to occur regardless of whether they are adversarial or not and also because I have already isolated Impact ranking to a different column )

(table explaining what numbers mean for impact)

()

~~But knowing that these threats and vulnerability is not enough, …after all, all assets have their own vulnerabilities and threats associated with them. Thus, we need to know how probable it is for the threat to take place and what the outcome will be for the company in case it does occur in order to truly understand their value or smth……(lookup quote by smbd who said this on google or smth)….This can be done by …link it to next part~~

Prioritization of Identified Risks:

---say that from the previous one, we can see that…..write the ranking order according to risk score found….. (with most significant being… and then… and…. And finally with the least one being…..)

---Then say, here you can notice that ….

(like if operation critical number matches the new risk order than say that it was surprising to see it match and this in turn assured us that we were on right track)…+++also say that due diligence had been done here by still following the protocols suggested to us by ……(whitmann, peltier and other articles where risk analysis or risk management process has been discussed---use the article that we had used in CLA#2)….have been followed

**OR**

(If operation critical number doesn’t match, then give rationale on why it didn’t match---like org considers these to be operationally critical, which in turn increases the impact of the risk (check out whether this line is supported by any defn of risk impact on either peltier, NIST, WHitmann, etc on google)---it has low likelihood of the risk materializing due to…. (maybe lack of necessary tool, expertise, access, grudge, etc…. look for all reasons likelihood can be low on google)+++also say that thus by not just relying on operation critical value and instead by going in depth and actually checking the risk, I have provided a more accurate analysis of the actual risk assosciated with the information assets and thus have done the “due diligence” (see if you had explained what due diligence means before, if you haven’t then explain it here now..) and thus can assure etricity that protocols suggested by……(whitmann, peltier and other articles where risk analysis or risk management process has been discussed---use the article that we had used in CLA#2)… have been followed

Conclusion

Now give reference to start by saying, Overall I had done…(risk assessment in terms of info sec on etricity )…and found that etricity was exposed to many risks, where the most significant 7 were noted in the report.

So what should etriciy do now? My suggestion and recommendation is for it do the following:

(note down the actions in bullet point like system and must take proper actions (like implement controls, plans, etc.---see what the reference article for part B in CLA#2 says about the things to do—only say their names and DO NOT ELABORATE!) in order to reduce, control and mitigate them, especially for….(note the risk that had highest RISK score) …which had the highest risk score, as soon as possible (+++ alongside…. (notable ones that either had relatively high impact or likelihood, but not at the top))

+++can also add the following line to end it, +++ at first encourage them with a quote saying ---tell them not be hopeless or overwhelmed or scared as they have taken the first step by asking me to carry out the risk assessment on their information systems and asset +++and also that it can contact me in case it had any issue regarding any of the information presented here or if they wish to discuss about the next steps they should take in details.

++ end the report with a quote from smbd online saying---not to be hopeless, already taking the first step away from ignorance and towards true security and protection which already quite good---or smth equivalent to it

++coutn the word limit till now, ignore words in all form of tables or executive summary, appendic or diagram or reference and only count the paragraph (at least make it 2000 words, max 2500 word)

(for word count not upto 2000, explain everything written in the table as paragraph form either above or besise it, especially in explaining the info in anakysing org critical valu, threa and vulnerability explaination, likelihood and impact explaination for each, etc…)

References---harvard style reference---link to the style: <http://www.swinburne.edu.au/lib/studyhelp/referencing.htm>

Proviti, eTricity case study, Iso31000:2018, Peltier, ISO27005:2012, Whitmann, NIST

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)