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 and brief explaination

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

EtricityAU (reference the case study) is company whose main focus lies on the production, installation and maintenance of PV (photovoltaic) solar panels for houses in Victoria. They do so by using an advanced monitoring system that tracks the performance and use of the solar panels in providing electricity to their customers and then by providing the customers with a live digital report regarding it (to help the customers fine-tune their consumptions and savings).

As the company grew in size to further expand into the market, it hired more personnel and divided the organization into various departments, each with their own roles and responsibilities. But, unfortunately, this growth had not resulted in bringing adequate number of skilled IT workers into the company, resulting in its old system (RecShareOne) being overrun with huge amount of data (customer, supplier, operational, etc.) without having proper number of people to maintain it.

This operational issue in turn has led to misunderstandings and miscommunications between the IT and business departments in the organization, creating various avenues of attack, some of which were exploited by DDOS attacks. This further increased the tension between the groups and had also resulted in several people from the IT team leaving the company (putting more pressure on the remaining ones)

All of these actions, alongside the rise in virus and targeted phishing attacks have led their Information System Manager to be concerned, resulting in me being assigned to perform an information risk assessment on their company.

In order to better understand what is it, one needs to understand what information security is. Following the words of Whitmann (reference), it is the “protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology”. This protection is maintained by analyzing the information assets in the organization, their vulnerabilities and threats in depth, categorizing and prioritizing them, and finally by using them to perform the risk assessment and management.

Here, in order to ensure that “due diligence” is being performed by me in my process (and hence assure the company), I am going to follow and state the proper protocols and standards each step of the way by defining what each factor is, identifying them, and explaining on how they all fit together in performing the process of risk assessment and management.

**[Note:** In order to perform Risk assessment, I am using the definition provided by ISO31000:2018 (reference) which identifies it as the process of risk identification, analysis and evaluation. And, in order to perform Risk Management, I am following the definition provided by same source (reference) which notes it as a list of coordinated activates in order to direct and control risks related to a company. ]

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

Before beginning the risk assessment process, it is better to keep the Strategic Environment, Risk Appetite and tolerance in mind as a baseline to follow. According to…. (<https://www.tandfonline.com/doi/pdf/10.3152/147154600781767303> ), strategic environment means analyzing the problems in organization’s environmental, noting the opportunities for organizational development, identifying main actors and defining strategic goals from the very start. Hence for Etricity, it is the production, installation and maintenance of the solar panel units for the customers in the Victorian domestic market, use of subcontractors in delivering and installing units, use of Guandong companies to manufacture unit components, etc.

Furthermore, according to Proviti (reference), Risk appetite is expressed using qualitative and quantitative statements to state the maximum acceptable performance variance and loss exposure that the business would allow, and Risk tolerance are the specific boundaries and parameters used to fulfill the risk appetite. Unfortunately, the company had not provided me with their Risk appetite and tolerance statement, leading me to craft the following statement from the information provided:

The company’s primary goal is to provide customers with proper production, installation and maintenance of solar panel units for customers in Victoria and ensure that the customers can get reports regarding it in real-time. Thus, their risk appetite should ensure that all risks to customers’ data are unacceptable. Furthermore, this should also extend to other organizational assets which are also business critical for their operational goal. But they seem to be willing to accept certain risks to ensure that their goals are met (like allowing subcontractors remote access to their systems, outsourcing manufacturing to external parties, etc). In order to better understand these, I have noted a few of the risks I noticed (along with their acceptable level) in the slider below:

Acceptable risk Not acceptable risk

* Lower product costs to sell fully assembled units
* Founders overriding their Board, design engineers and business manager’s decisions
* Setting tenders to selected suppliers for products that has technical specification
* Performing important business tasks on personal device and ignoring the ‘IT guy’
* Keeping recShareOne running with patches, extensions and workarounds
* Not knowing where data is being stored
* Loss of reputation as market leader
* Putting national compliance in terms of the developed product at risk
* Keeping original designs in RecShareOne (company’s custom-made enterprise system)
* DDOS attack on company server and phishing attack on account details
* The new solar and customer information platform
* Customer’s data’s confidentiality, integrity and availability being compromised
* Allowing subbies (sub contractors) to distribute and install the units and access the enterprise system remotely
* Reusing old documents and templates which are unique to company
* Sharing architectural designs and plans with business partners
* Outsourcing manufacture of general component to external parties
* Lack of proper, skillful IT staff

Roles and Responsibilities Identification

Now that a baseline for the risks that the company is willing and not willing to take has been developed, it’s time to analyze the roles and responsibilities of people in the organization as according Peltier (reference), “risk management is an enterprise management responsibility” where everyone have different roles and responsibilities which support each other in regards to risk analysis and management. So, I have noted down the roles and responsibilities of the people in the company below:

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Owners (Brad Hill and Angelique Farelli) | Monitoring and managing risks related to information systems and assets, designs, research, development and innovation areas  Preparing proper risk, control and governance framework to prevent clash between different groups  Ensuring that proper risk management steps take place in the organization |
| Chief Financial Officer (CFO) Josh Fraser | Managing the information regarding the financial situation of the company and passing proper planning to BOD, Owners, etc. |
| Board of directors (BOD) | Being aware of all Information system’s and asset’s risks, their impacts and the effective ways to manage them (including reducing risks in old system, shifting to new system, etc.) |
| Business Managers | Being aware of risks, impacts and mitigation methods for the information assets and systems under their control and managing it |
| Subbies (subcontractors) | Ensuring to use secure devices and communication channels (like company VPN) while remotely accessing company’s information assets and systems |
| Information System Manager(ISM) Alain Monte Perrie | Being aware of all risk and security issues regarding all information system and assets being utilized by the company and managing it. |
| Chief data officer (CDO) Jock Jorden | Being aware of all risk issue regarding data system and managing it, especially the new etricity au data warehourse |
| IT department (Database administrators, data entry clerks, programmers team, etc.) | Being aware of all risk and security issues regarding all information assets (like all data entered into RecShareOne, Etricity AU Data warehouse)and managing it  Ensuring proper maintenance is being performed onto systems (like on RecShareOne and Etricity AU Data warehouse) |
| HR Manager (Rebecca Adams) | Being aware of all risk and security issues of having HR data stored onto Cloud systems |
| Customer Service Manager(CSM) Theresa Alvantez | Being aware of all risk and security issues of having HR and Customer service data stored on “Work.com” |
| design engineers | Being aware of all risk and security issues of all data related to designing, building and testing the prototype system and managing it |
| Chief Engineer (CE) Felix South | Being aware of all risk and security issues of all data being between the suppliers and the company and managing it |
| Accounts reconciliation officer (ARO) Sally Brent | Being aware of all risk and security issues of banking and accounts data and managing it |

Whilst reading, I have also noticed some risky actions which they had performed and analysed them:

|  |  |
| --- | --- |
| Actions performed | Why it is risky |
| Angelique keeping original design documents in wooden cabinet | This exposes those documents to natural disasters like fire, flood, etc., over time degradation of paper, and also removes them from backup and recovery methods which are present for documents stored digitally |
| Angelique and Brad overriding their BOD, design engineers and business manager’s decision | Although they have “superior understanding” of technology from past year, this does not necessarily make them fully prepared to deal with all current and new issues on their own |
| CFO wanted to lower costs to sell fully assembled units internationally | Lowering the costs usually leads to cutting corners in product, increasing chance of malfunction and thus loss of company reputation |
| BOD being ignorant about issues with RecShareOne due to lack of any directly report to them about it by ISM | This makes them unaware of how serious the issue is and thus results in them not being prepared to handle any crisis that it may lead to |
| ISM not having enough direct authority  (eg CSM considering him as a “IT Control freak” with no power) | ISM is supposed to be responsible for the entire organization’s security and risk aspects and thus not giving them the authority results in theirs warnings not being heeded |
| ISM delegating backup task to a new company owned by his friend | Since a competitive process had not been performed to select the backup company, there is no guarantee that the external, new company can actually backup the huge amount of data properly (and also retrieve it if needed) |
| CDO not knowing about legacy system | Since the company is currently using and depending on a legacy system (RecShareOne), and thus not knowing details about it would lead to him being unable to properly deal with issues regarding that system |
| ARO not listening to CDO and keeping important business files on her personal desktop | Since it is not a company device but instead her own, there is no guarantee that proper security measures have been taken in order to protect the business files |
| HR Manager not considering issues in offshoring HR data | Since data is kept offshore, there is no guarantee that proper security policies (like privacy laws, anti-theft measures, etc.) are going to be followed, increasing chances of data loss and compromise |
| CDO not defining proper policies on how new system’s operations will be used by the different departments (like Customer Service team) | This makes it difficult for the departments to utilize the system to its fullest and also leads way for issues in tasks allocation, miscommunication between the departments, both of which in turn lead to issue in information asset’s security |
| CSM not consulting with ISM about using the new system (Work.com) to handle HR and Customer Service data | CSM doesn’t necessarily have all the technical expertise and experience needed to ensure whether the new system is actually providing proper security features towards the information assets and system, but ISM does. Thus it would be better for her to consult with ISM before proceeding with the new system |
| CE not following proper competitive tender process in selecting suppliers | This means the suppliers chosen may not necessarily have the proper expertise needed to produce quality product. Also they may not utilize the proper security measures in protecting the data (like special component design) that they received from the company |

**Note:** Here I am not including manufacturing and assembly companies from Guangdong, construction companies from Melbourne and the Specialist Company in Wonthaggi as these are part of third party organizations and thus not considered as internal people of Etricity.

Information Assets Identification

Throughout the report I have continuously been using the word “Information Asset”. This is basically any information resource that is valued by the organization (like customer details, research data, invoices, business policies, etc.) (reference—week1slide—pg28) and hence is usually the main point of attack on any business.

Thus, in the following table, I have identified the Information assets of the company and noted their value (detailing what each value classification means in the table just below that):

**Note:** Here I am not considering eTricStorage’s intelligence system as part of the major IT systems as it is currently only used as trial on a small number of customers and thus doesn’t handle much data, unlike RecShareOne and the Etricity AU Data warehouse.

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset Name** | **Asset Storage** | **Asset details** | **Value of Asset** |
| Reports Data | Data Center | Informs customers how much electricity they are producing and using | High |
| Customer Data | Data Center, Data warehouse | Contains the personal information of customers (like their name, address, credit card details, etc.) | High |
| Transactional Data | Data Center, ARO’s own device | Contains banking information (like billings, invoices, etc.) | High |
| Operational record data | Data center | Contains information about all business process (like contractor information, supplier details, order details, etc.) | High |
| HR and Employee data | Data center | Contains personal information of employees (like their name, address, credit card details, etc.) | Medium |
| Major IT systems (RecShareOne, Etricity AU Data warehouse) | Data center, Data Warehouse | Contains all information assets stored into them | High |
| Research Data | Data center, Data warehouse | Contains all research and innovation data (like domestic lithium battery technology) | Medium |
| eTricStorage intelligence system’s real time data | Data center, Data warehouse | Contains real-time information about the customer’s electricity usage, storage, current electricity prices, etc. | High |
| Project data | Data center, Data warehouse | Contains all current project details (like designing, testing prototypes, etc) | High |

|  |  |
| --- | --- |
| **Value of Asset** | **Meaning of the Rank** |
| High | * Asset critical to success of the organisation * Asset generates most revenue and profit, * Asset most expensive to replace or protect, * Loss or compromise of asset leads to greatest liability or embarrassment |
| Medium | * Asset moderately important to success of the organisation * Asset generates moderate revenue and profit, * Asset moderately costly to replace or protect, * Loss or compromise of asset leads to moderate liability or embarrassment |
| Low | * Asset of little important to success of the organisation * Asset generates little revenue and profit, * Asset cheap to replace or protect, * Loss or compromise of asset leads to little or no liability or embarrassment |

**Note**: In order to set the meaning of rank, I have utilized Whitmann’s 6 questions (refernece) for determining value of asset.

Threat, Vulnerability and Risk Identification

Now that all the information assets have been identified, it’s time to consider the vulnerabilities and threats associated with those assets, in order to identify the risks present in the organization. Here, I am following the definitions provided by Whitmann (reference). which states Vulnerability as a potential weakness in asset or system and threat as a potential risk (or loss of value) of an asset. Or, in simpler terms, vulnerability is the weakness inherently present in the information asset and threat is the harmful outcome (ie the risk) that this vulnerability can lead to.

Unfortunately, each assets have multiple vulnerabilities and threats and it is not possible to go through and prepare to each and every case scenario. So, in this report, I am only going to speak about the 7 most important ones using the OCTAVE table (Operationally Critical Threat, Asset, and Vulnerability Evaluation) which is supported by Whitmann (reference).

**Note**: Here, the following 7 are all operationally critical and the current ranking is done just to order them relative to one another. Furthermore, in order to identify proper threat and vulnerabilities of those assets, I am utilizing both Whitmann(reference) and also ISO27005:2012 (reference).

|  |  |  |  |
| --- | --- | --- | --- |
| **Operationally Critical Number** | **Threat** | **Asset** | **Vulnerability** |
| 1 | Software Malfunction, Equipment failure, breach of system, DDOS (Denial of service attack), etc due to old system not being able to handle the load of all the information | Operational Data in RecShareOne | Old system made by local company that no longer exists and is instead running on continuous patches and workarounds  Also, lack of adequate number of IT staff skilled on this system |
| 2 | Forging of user rights and user errors in use, both of which can lead of corruption and theft of data | Reports data | Poor password management and lack of security awareness |
| 3 | Corrupted or fraudulent data can be passed directly to system by disgruntled subbies, leading to system malfunction | Customer’s data | Subbies’ accessing those information (like customer name, address, email,etc.) remotely on thier BYODs |
| 4 | Information compromise via eavesdropping or remote spying due to lack of adequate security measures (like data being transferred over insecure lines) on ARO’s devices | Transactional data | ARO storing and processing those information (like ledger, banking details, etc.) on personal laptop which is not secure |
| 5 | System Malfunction, Errors in use can cause loss of service or breach of information | eTricStorage intelligence system’s real time data | It is an immature or new software that is still on trial process with small number of customers |
| 6 | Software Malfunction, Equipment failure, breach of system, DDOS (Denial of service attack), Errors in use,etc. can cause loss of service or breach of information | Major IT systems (RecShareOne, Etricity AU Data warehouse) | Old system issues for RecShareOne, and proper policies not being set by CDO on Etricity AU Data warehouse |
| 7 | Loss of data due to improper backup, data breach, abuse of rights, corruption of data, theft of data, etc. can occur as the data is being backed up by unreliable source and also because data is being accessed by personnel who haven’t gone through proper vetting | Project data | Backups of the data are being done by small company run by a friend of ISM and thus haven’t been properly tested.  Also, suppliers who have access to those data have been assigned by CE without following proper competitive tender process |

Likelihood and Impact of Risks

Since the top 7 operation critical assets, threats and vulnerabilities have been noted, these can be used to understand the most important risks that are currently present in the company. But even so, this information does not help fully understand the severity that these risks pose. So, in order to accomplish that, I am following NIST’s process (reference) where risk is considered as a function of likelihood of a threat event occurring and the potential adversarial impact that it would have when it occurs. Furthermore, it also defines likelihood to be a weighed risk factor that is determined by analyzing the probability of a given threat being capable of exploiting certain vulnerability, and impact as the magnitude of harm that the outcome can result to as the consequence.

Thus, I am going to expand on the previous table by including the likelihood and impact of the risk for each case.

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

1. the critical number is currently uniquely identifying them,
2. it makes the information in the table more easier to read and understand

**Note**: Here, “Risk Score = likelihood Score \* Impact Score”. Also, the meaning behind the scores for likelihood and impact have been noted in the table below, using the ranking scale provided by NIST (reference)

|  |  |  |  |
| --- | --- | --- | --- |
| **Operation Critical number** | **Likelihood score**  **(1-100)** | **Impact score**  **(1-100)** | **RISK Score**  **(1-10,000)** |
| 1 | 80 | 95 | 7600 |
| 2 | 81 | 96 | 7776 |
| 3 | 83 | 97 | 8051 |
| 4 | 60 | 95 | 5700 |
| 5 | 84 | 40 | 3360 |
| 6 | 96 | 98 | 9408 |
| 7 | 50 | 90 | 4500 |

**Note:** Here in the likelihood table, I have merged NIST’s likelihood scale of threat event occurrence both due to adversary and natural causes together and have not included the information considering chance of having adverse impact. That’s because here, risk for the threats noted in etricity can occur both due to human intervention and due to natural causes, and the fact that all of them are guaranteed to cause adverse impact on the company.

|  |  |
| --- | --- |
| **Likelihood Score** | **Meaning** |
| 96-100 | i) Adversary is almost certain to attack,  ii) Error accident or act of nature is almost certain to occur, or occur more than 100 times a year |
| 80-95 | i) Adversary is highly likely to attack,  ii) Error accident or act of nature is highly likely to occur, or occur between 10-100 times a year |
| 21-79 | i) Adversary is somewhat likely to attack,  ii) Error accident or act of nature is somewhat likely to occur, or occur between 1-10 times a year |
| 5-20 | i) Adversary is unlikely to attack,  ii) Error accident or act of nature is unlikely to occur, or occur between less than a year or more than once every 10 years |
| 0-4 | i) Adversary is highly unlikely to attack,  ii) Error accident or act of nature is highly unlikely to occur, or occur between less once every 10 years |

|  |  |
| --- | --- |
| **Impact Score** | **Meaning** |
| 96-100 | The threat event might cause multiple:  (i) severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;  (ii) major damage to organizational assets;  (iii) major financial loss;  (iv) severe or catastrophic harm to individuals, including loss of life |
| 80-95 | The threat event might cause at least one:  (i) severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;  (ii) major damage to organizational assets;  (iii) major financial loss;  (iv) severe or catastrophic harm to individuals, including loss of life |
| 21-79 | The threat event might cause:  (i) significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but not effectively;  (ii) significant damage to organizational assets;  (iii) significant financial loss;  (iv) significant harm to individuals, without any loss of life |
| 5-20 | The threat event might cause:  (i) degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but slightly less effectively;  (ii) minor damage to organizational assets;  (iii) minor financial loss;  (iv) minor harm to individuals |
| 0-4 | The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. |

Prioritization of Identified Risks and brief explaination:

So, following the Risk Score, it can be seen that the most significant risk lies in Major IT systems, then Customer’s data, then Reports data, then Operational data, then transactional data, then project data and finally the ETricStorage intelligence system’s real time data. Although it doesn’t match the initial operation critical number that had been determined in OCTAVE table, it is easy to understand why. That’s because:

a) Major IT systems currently handle all the data being used by the organization, accessed by several people and uses both extremely old and brand new softwares. Thus it has extremely high chance of being attacked and also an extremely high effect upon being attacked,

b) Customer data contains all customer details and is accessed by several subbies in their own devices where proper security protocol may not be implemented (and also disgruntled subbies may purposefully cause issue). Thus it has a significantly high effect and also high chance of being attacked,

c) Reports data contains all the information regarding the electricity production, usage,etc by the customers and is one of the main business objectives and is accessed by customers. Thus although it has similar high effect as Customer data, it has a lower chance of being attacked.

d) Operational data in RecShareOne contains all information about business processes (like contractor information, supplier data, order information, etc) accessed by trusted, internal employees of the company using company’s devices. Thus, although it has a similar high impact as the reports and customer data, its chance of occurring is lower (as they are accessed by using devices that have good security features maintained in them and by employees who know what to do and not do),

e) Transactional data stored by ARO on their own devices and contains sensitive business information like banking details, invoices, etc. Thus it has an extremely high impact. But since it is being accessed by only a single person, the likelihood of the attack is low, compared to Operational, Reports and customer data,

f) Project data contains all details about current prototype design, innovation, testing details, etc and is accessed by suppliers who may not have been properly vetted by the CE, alongside not being properly backed up. Thus, it has a high impact, but not as high as those affecting Transactional data as although project data is important, it is not more important than the ones listed before it. Furthermore, its likelihood is lower than one for transactional data as these suppliers (and also ones taking backups) are also part of different companies who can ensure proper security features are being maintained,

g) eTricStorage intelligence system’s real time data is a brand new system being used on trial basis on a small number of customers and has live information about the customer’s electricity usage, storage, current electricity prices, etc. Thus although it is highly likely to be attacked (as it’s a brand new system), its impact is quite less as it is only being used by a small group of customers

Conclusion

Overall, in this report, risk analysis have been performed on Etricity using the processes and protocols adviced by Whitmann, Proviti, Peltier and Paul, and also using standards followed by ISO31000:2018, ISO27005:2012 and NIST (in order to fulfill due diligence in risk analysis). This has resulted in the detection of various risks that currently exist in the company, alongside detailed analysis of 7 most significant ones.

So, now that the major risks have been found, what should the company do?

I would recommend the company to do the following:

1. provide detailed risk appetite and tolerance to better understand which risks the company is willing and unwilling to take,
2. go through the report once more and perform an internal inspection on the information assets and their risks (especially against the 7 most critical ones) and then take appropriate risk mitigation strategies (like implementing controls, plans, etc.) against each, in order to reduce, control and mitigate the risks.

Furthermore, although the situation is quite serious (considering the scope of issues that could pop up and the miscommunication between the IT and business departments that have already been created by it), the company should not feel hopeless, overwhelmed or scared. After all, by asking me to perform risk assessment on their information assets and systems, they have already completed 50% of risk management according to ISO31000:2018 (reference) and Paul (reference) *[see in the diagram below].* Moreover, the company can also contact me later on, in case any clarification is needed for any of the information noted here in the report or if they wish to discuss about the next steps they should take (ie risk treatment steps) in details.

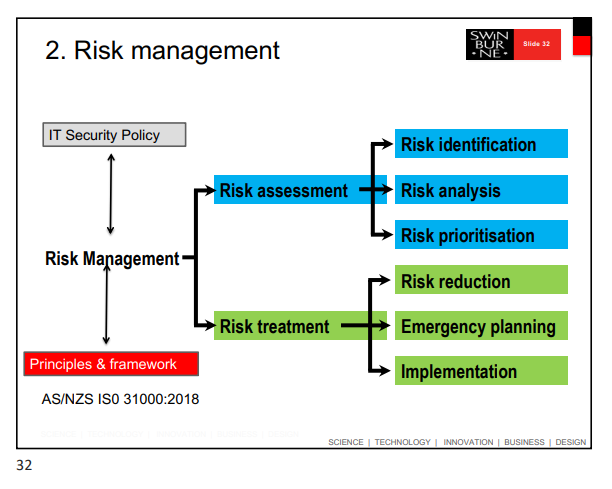


Figure: Risk Management Process given by Paul and supported by ISO 31000:2018

Contact me to mitigate the risks before they lead to crisis or clash between departments which lead to crisis etc.

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.---say that these have been done using……all reference names…

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…)

Moreover, the final risk score had been obtained following methods of

Thus, although the Operation critical number does not match with the risk score ranking outcome, the risk score ranking is more accurate to be used in prioritizing the risk as it follows the risk analysis processes followed by Whitmann, NIST, Peltier, …. And so ensures that due diligence have been performed byme

(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

---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

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)