Course name: Information Systems Risk and Security
Course ID: INF30020

Name: S M Ragib Rezwan
ID: 103172423

Title: Risk & Security Management Report A (Individual)

Content list:

Executive summary

EtricityAU is a company who specialized in producing, installing, and maintaining photovoltaic (PV) solar panel solutions for homes in Victoria. It had been established in 2012 in Inverloch, Bass coast, Victoria, Australia by Brad Hill and Angelique Farelli from Swinburne University of Technology's Information system.

Although the company has taken several steps (like in the introduction of Etricity AU Data warehouse and EtricStorage systems, hiring of new people to the company, etc.) in order to grow and accommodate a large number of customers, not all of the proper steps have been taken (like not hiring more IT people, not properly vetting the process by which suppliers were being, not creating proper policy for the new systems' use, etc.) . This in turn has led to several misunderstandings and miscommunications between various groups (Information Technology (IT) department, Business department, Human Resources (HR), Board of Directors (BOD), Owners, etc.) which in turn led to several security issues, attacks, etc. further increasing the tension between them.

Noticing all of these, the company has assigned me the task of creating a risk assessment report in order to analyze the threats, vulnerabilities and risks in the information assets and systems present in the company in order to identify the major risks and proceed towards mitigating them.

Hence in this report, I have explained my approach to Information security risk management and risk assessment (letting the company know my understanding of risk and its related terms), defined and described their strategic environment along with a possible risk appetite and tolerance (which I had inferred from the case study) and explained and noted the roles and responsibilities of people in the organization (alongside the risky actions that they had taken), the information assets present in the company, the threats and vulnerabilities associated with the 7 most critical information assets, likelihood and impact of the risks associated with them (alongside the risk score). Finally I have also concluded noting the reference materials I have used and my rationale behind them, alongside brief recommendation on the steps the company should take now that the most critical risks have been identified.

[**Note:** *Although I have mentioned about risk management and what it is in brief, I have limited my report to risk assessment part of it only and thus, have not included risk treatment steps*]

Introduction

EtricityAU 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 risk assessment means, one need to understand what information security is. Following the words of Whitmann and Mattord **(2019, p.2)**, 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* ***(2018, p.11)*** *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* ***(2018, p.1)*** *which notes it as a list of coordinated activates in order to direct and control risks related to a company.*]

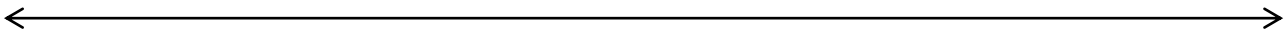
Strategic Environment, Risk Appetite & Risk Tolerance

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 Kessler **(2012, p.295)**, strategic environment means analyzing the problems in organization's environment, 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 Protiviti **(2012, p.1)**, 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 **(2012, p.9)**,. 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

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

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 **(2004, p.46)**, "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:

[Note: *Here I am not including manufacture 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*.]

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 systems' and assets' 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 using 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 prototypes and managing them
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 analyzed 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 adequate authority results in their 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), 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

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.) **(Paul, 2022)** 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,	Contains banking information (like	High

	ARO's own device	billings, invoices, etc.)	
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 the information assets of the company stored into them	High
Research Data	Data center, Data warehouse	Contains all research and innovation data (like domestic lithium battery technology, etc.) of the company	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.) of the company	High

[**Note**: *In order to set the meaning of rank, I have utilized Whitmann and Mattord's 6 questions **(2019, p.260-261)** for determining value of asset.*]

Value of Asset	**Meaning of the Rank**
High	• Asset critical to success of the organization • 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 organization • 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 organization • 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

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 and Mattord **(2019, p.9)** 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 (i.e. the risk) that this vulnerability can lead to.

Unfortunately, each asset has 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 and Mattord **(2019, p.309).**

[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 and Mattord* ***(2019, p.264-269,279)*** *and also ISO27005:2012* ***(2012, p.42-48).***]

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 that 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 their BYODs
4	Information compromise via eavesdropping or remote spying due to lack of adequate	Transactional data	ARO storing and processing those information (like

	security measures (like data being transferred over insecure lines) on ARO's devices		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 **(2012, pg.6)** 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 **(2012, pg. 10)**, and impact as the magnitude of harm that the outcome can result to as the consequence **(2012, pg. 11)**.

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:*

a) the critical number is currently uniquely identifying them,
b) it makes the information in the table more easier to read and understand

*Furthermore, 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* **(2012, pg. G2, H3)**.]

Operation number	Critical	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 instances of: (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 a single instance of: (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 explanation

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 software. 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 advised by Whitmann, Mattord, Proviti, Peltier, Kessler and Paul, and also using standards 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:

a) provide detailed risk appetite and tolerance to better understand which risks the company is willing and unwilling to take,

b) 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 Paul **(2022)** *[see in the diagram below].*

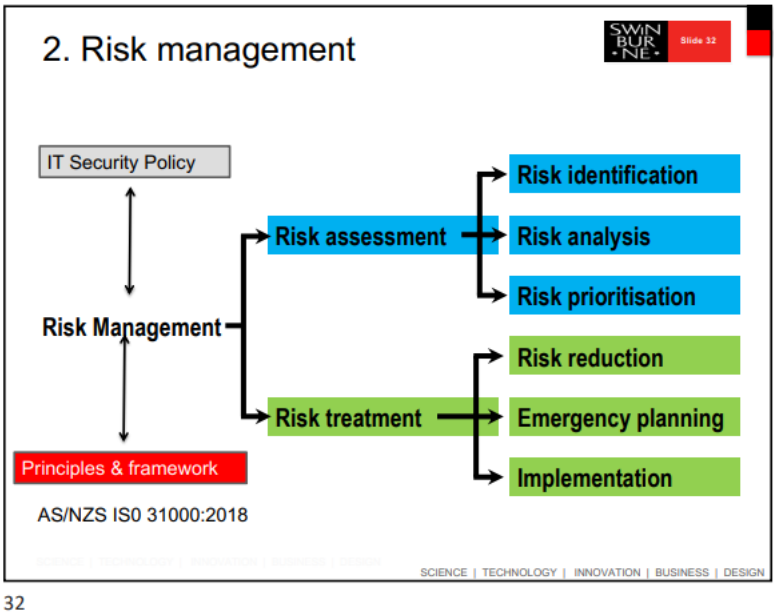


Figure: Risk Management Process given by Paul **(2022).**

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 (i.e. risk treatment steps) in details.

Reference

a) Whitman, Michael E. and Mattord, Herbert J. 2019, *Management of information security*, Sixth Edition, Cengage Learning, Stamford, Conn.

b) Standards Australia 2018, *Risk management - Guidelines*, (AS ISO 31000:2018), Techstreet Enterprise.

c) Kessler, Joost J. 2000, 'Strategic environmental analysis (SEAN): a framework to support analysis and planning of sustainable development', *Impact Assessment and Project Appraisal*, Vol. 18, no.4, pp. 295-307.

d) *Defining Risk Appetite* 2012, Protiviti, [unknown place of publication].

e) Peltier, Thomas R. 2004, *Risk Analysis and Risk Management,* Information systems security, [unknown place of publication].

f) Scifleet, P. 2022, 'Introduction and Overview: IS risk and security', INF30020 Information Systems Risk and Security, Learning materials via Canvas, Swinburne University of Technology, 1st Aug, viewed 1st Aug 2022.

g) Australian/New Zealand Standard™ 2012, *Information technology—Security techniques—Information security risk management (ISO/IEC 27005:2011, MOD)*, (AS/NZS ISO/IEC 27005:2012), Techstreet Enterprise.

h) National Institute of Standards and Technology (NIST) 2012 Guide for Conducting Risk Assessments, *(*NIST Special Publication 800-30 Revision 1*)*, Techstreet Enterprise.