Final Year Project – Cyber Insurance Application

Research manual

Dermot Berry

South East Technological University

17/04/2023

Table of Contents

1 Introduction

For my project, I have researched third-party vendors' security. No matter how safe you feel, your IT security is only as secure as your weakest link. In most IT companies their weakest link would be their third-party vendors. Ackerman Jr., (2022) states that "as a result, the risk of a cyber-attack for SMBs – already typically higher than the risk for big companies – has grown dramatically over the past couple of years. During 2020 and 2021, data breaches at small businesses globally soared 152% compared to the previous years." Along with the significant number of breaches, over half of them can be detrimental to a small-medium business (SMB). As stated by (Comerford, 2022) "60% of all small business victims of a data breach permanently close their doors within six months of the attack."

When trusting a third party with company information, you are trusting that the vendor will help keep your integrity and confidentiality. During my research, I discovered that vendors place a lot of trust in third party suppliers, and companies assume that they have the necessary policies in place to ensure Confidentiality, Integrity, and Availability (CIA). (SecureLink 2021) pointed out that "65% of third parties are not required to fill out security questionnaires, and shockingly, even more - 74% - are never asked to conduct remote or on-site assessments".

From my observation, it became evident that vendors' security postures vary widely and are susceptible to multiple security breaches. With an application to access their security controls in place, this describes how third-party vendors are prepared for any incident. The vendor is assessing if a third party can be "trusted" when providing a service to the vendor. After understanding why there are so many gaps in these systems, I intended to develop an application using a scoring system to assess third-party vendor security for vendors who are currently using a service or who are searching for a new service provider. However, as I describe in Section 4, it was more appropriate to change the focus of my application to create an application that enables insurance companies to gather information from organisations seeking cyber insurance. The information is automatically assessed to determine if the insurance company should accept the risk.

2 Current Risks to Vendors

In recent years there has been a global shift in the work environment, due to the pandemic starting in 2019 it caused almost all businesses in some capacity to move some if not all their business online to keep revenue coming in and to prevent job losses.

However, this came at a price in the IT security sector. Most businesses did not have a remote working policy in effect and with covid 19 it shifted everybody online quickly, this led to several security threats. According to (Redcentric.com, 2022) there are 5 top security risks of remote working.

1. GDPR and Remote Working
2. Phishing Emails
3. Weak Passwords
4. Unsecure Home Devices
5. Unencrypted file sharing

GDPR would have been affected as there were people who may have been using their own devices and storing user data locally. This became a critical risk as most users would use weak passwords on their devices, their home router admin password also may not have been changed to a more secure version, this made it much easier to access their locally stored data. In 2020 the there was a substantial increased number of phishing email attacks according to (Warburton, 2020) “phishing incidents rose by a staggering 220% compared to the yearly average during the height of global pandemic fears.” As we can see with the above example, this is only one area where there may be a risk to all companies due to changing to a remote working environment. You may see areas of the business that are adequately secured however, in this one instance, there are many risks relating to working remotely. With remote working, employees are less inclined to worry about security and feel they won’t be breached at home. During covid many businesses suffered from the loss of intellectual property due to several factors. One of these factors are threat actors accessing online meetings under a different alias. Another threat is people who record online meetings e.g., somebody recording your presentation to potential clients and using it for personal gain. Confidentiality is a major concern as employees would often leave their devices open while working remotely, which could lead to shoulder surfing from social engineering etc. As pointed out by (Purplesec, 2022) “Remote work has increased the average cost of a data breach by $137,000”. While working remotely does the employer have the end devices fundamentally encrypted? Has the employer the ability to lock the laptop remotely, or further, wipe the device remotely. These are risks that smaller vendors may not have taken into consideration. Will the third party provide certificates which are applicable such as ISO 27001 or SOC 2 compliance? Will they use best practises standards for compliance such as HIPPA? PSD2 compliance? Will the vendor deal abide by GDPR Standards. Small vendors dealing with financial, health etc must have GDPR in place. According to (Enisa, 2022) “After all, an increase in cyber defences becomes fruitless if attackers have pathways directly into organisations via compromises of third-party relationships”.

With IT security being a broad area with a plethora of topics, it is paramount that the client is satisfied with the security controls in place by the vendor. There is no business that is fully secure,

with technologies constantly evolving there will always be risks. Carrying out security assessments gives assurance to all parties to outline the cyber posture of the vendor.

2.1.1 The need for third party security reports/assessments

According to (Omer, 2022) “Over 84% of inspected third parties used Google as a fourth party” (see Fig. 1.). This shows that any company using Google in any form for their cloud services may be vulnerable to their business being compromised if there has been a disruption in services, which could lead to a loss in both services and income.

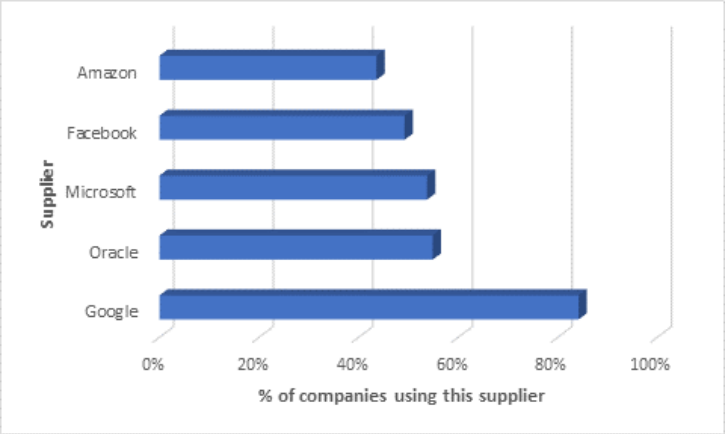


Fig 1: Companies using suppliers (2019)

2.1.1.1 Deloitte Report: Third-party governance and risk management

The need for an increase in third party vendor’s security in the IT sector is seen everywhere as stated by (Park & Sen, 2016) “the nature of the tasks being executed through third-parties is becoming more critical than ever before, thus increasing the severity of consequences on disruption or failure”. As seen in 2016, it was becoming a vital part of the cyber posture of IT companies and the demand for secure third-party suppliers remains higher than ever.

Vendors constantly share their data with third parties as stated by (Donohue, 2022) “Organizations rely on third parties for everything from cloud hosting to SaaS software solutions to business

partners and providers. 82% of organisations also share all their cloud data with these third parties, which creates risk for both negligent and malicious breaches". This reinforces the need for vendors to require assurance from third parties that they have a policies and controls in place to protect them from a loss of services etc.

There is a knock-on effect when a vendor suffers a breach. As a result of the breach, it may carry over to their third-party clients and in turn spread further. Implementing a scoring system would assure clients that their third-party vendors would have a good cyber posture in place and intrust the third-party vendor with client data etc.

2.1.2 Use cases showing the repercussions of third-party vendor security.

2.1.2.1 SolarWinds

The SolarWinds attack is a great example of the importance of third-party IT security. This attack occurred in 2020 where their system "Orion" was breached. Their customers included the Pentagon, Department of Energy Hospitals, Cisco, Microsoft, and many other large entities. During this attack (Jibilian & Canales, 2021) "SolarWinds told the SEC that up to 18,000 of its customers installed updates that left them vulnerable to hackers." 18,000 businesses had malicious code installed onto their own systems by means of an update, which in turn effects all the devices and networks that they relate to. It was one of SolarWinds customers FireEye who first discovered the attack on their own system. FireEye's own internal tests detected the attack which led to the threat being detected. It is estimated that it may take several years to fully recover from the attack.

2.1.2.2 Kaseya breach

On the 2nd of July 2021 Kaseya suffered a ransomware attack which affected 0.1% of their customers. Kaseya provide software solutions to MSPs (Osborne, 2021) and "800 to 1500 small to medium-sized companies may have experienced a ransomware compromise through their MSP". This shows that a substantial number of third parties are involved directly and effected by it. As a result of this many MSPs had to turn off their servers so that Admin access didn't get locked out. During the attack (Writer, 2021) "The Swedish Coop grocery store chain closed all its 800 stores on Saturday".

In another instance one customer had to shut down their stores which then affected hundreds and maybe thousands of customers, causing a loss of income and downtime. This created a snowball effect which could have been prevented by improving cyber posture and undertaking due diligence.

In conclusion the attacks were quite similar as third parties from both organisations were compromised, from the Pentagon to a Swiss co-op chain and the full effect of these attacks has not been uncovered yet. It is almost impossible for these vendors to disclose whether their business will ever fully recover their Integrity from these attacks. MSPs that used Kaseya now have legitimate reason to be distrustful of their own third-party vendors.

3 Small Medium Business (SMB) IT Security Risks

During the pandemic, small and medium-sized businesses were forced to relocate to the online environment to survive. In doing so business revenue online skyrocketed. Despite the market's slowing down according to (Almack, 2022) "e-commerce revenue is still up by 121% vs. the same period in 2019." With such an increase in online traffic it also entices threat actors to take advantage of the current IT security of small to medium businesses. It is paramount that these small businesses invest in fundamental IT security given the increase of revenue. After a compromise, these vendors typically bolster their security to some extent. (Coker, 2022) stated that "nearly all respondents said their organisation took cybersecurity much more seriously after experiencing a breach". As the internet grows and its services grow, so does the amount of risk to vendor IT security. One of the reasons of neglect is that businesses are unaware they have been compromised. Another major reason for neglect is human error as pointed out by (Osborne, 2022) that
in managing threat detection and response, it's important to take into consideration human factors such as mistakes, a lack of cybersecurity, awareness or training, or deliberate activities.

3.1 Improvement of SMB Cyber Posture

As SMBs wish to gain a positive reputation with potential clients to access more revenue, channels, client business etc., it is therefore critical that they increase their security posture.
Even if these companies might not have the funding or resources to increase security significantly, there are still ways to do it with a relatively small investment or simply add multiple-factor authentication to access emails which is available at no cost to the vendor.

- Modify existing passwords and increase the complexity.
- Keep devices up to date.
- Make backups.
- Implement a plan in the event of a breach.
- Use Multi Factor Authentication (MFA.

3.1.1.1 Third Party due diligence

According to (Cronley 2019) "Due diligence in Information Technology (IT) is to identify potential risks not obviously apparent and to verify information provided by vendors. When a third party is exploring how much they are undertaking to show their due diligence it shows various aspects, it will

uncover their liabilities, their risks, and their own performance. Cronley also points out that when undertaking due diligence, the vendor can see how vulnerabilities are reviewed and what steps are taken to mitigate them".

4 Change of Project Direction

During my research, I realised that my project would benefit from changing my application to a cyber insurance application. This allows the application to be tailored for use in the Insurance sector. According to (Enisa, 2023) "26 % of the respondents currently have cyber insurance and 74% do not." (See Fig. 2).

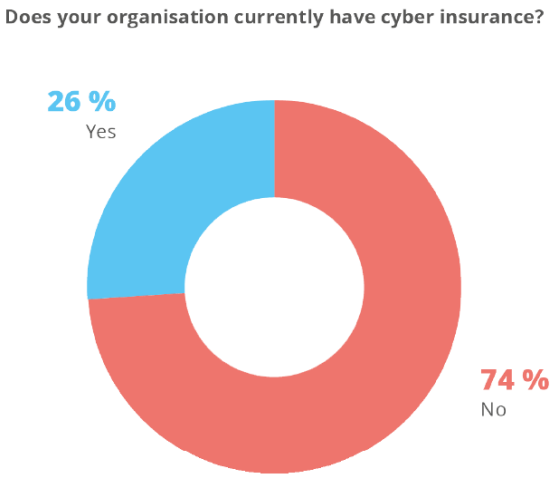


Fig 2. Uptakes of Insurance in the respondents

The pandemic has played a major role in the increase of cyber-attacks, as stated by (Lyons, 2020) "Google says it saw more than 18 million daily malware and phishing emails related to COVID-19 scams just in the past week." Phishing emails are only one entryway into a business's infrastructure which may lead to devastating consequences without acquiring insurance prior to an attack. Attacks in recent times have increased globally, which demonstrates the importance of cyber insurance. According to (Carson, 2023) "The cyber insurance market is expected to reach $20.6 billion by 2025" (See Fig 3). This is a significant increase, which Carson states that it's an increase $7bn from the same time in 2020.

Commented [CS1]: basically, whenever you have a figure you should reference it from the text. I haven't marked up any more.

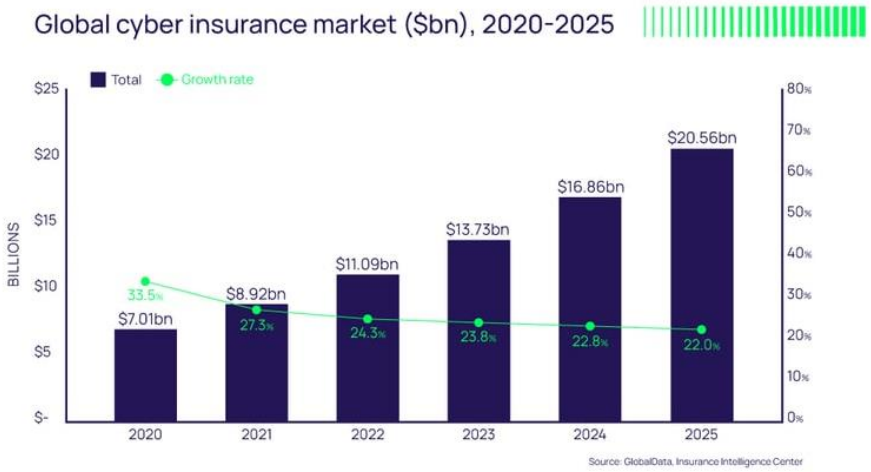


Fig 3: GlobalData, Insurance Intelligence Centre figures according to (Carson 2023)

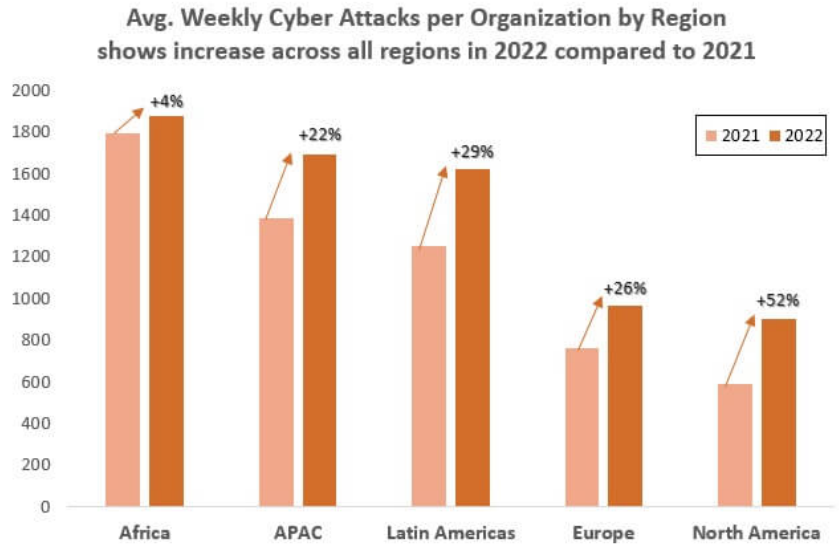


Fig 4: (Research Team, 2023) Increase of cyber-attacks in 2022 compared to 2021 globally.

In my opinion businesses are now starting to take cybercrime seriously, showing that cyber insurance is as essential as property insurance. Statistics according to (Rahmonbek, 2023) "In 2020 alone, there were over 700,000 attacks against small businesses, totalling $2.8 billion in damages. ", That many attacks on small businesses can be detrimental as Rahmonbek also stated that "Just 17% of small businesses have cyber insurance" and that "48% of companies with insurance did not purchase it until after an attack." These statistics are unnerving as most customers in some shape of form deal with small businesses on a regular basis which involves providing their sensitive data to the business.

5 Cyber Risk in Ireland

As stated by (ERM Financial Services 2022), "Phishing and ransomware are the most common types of cyber-attacks, with ransomware costing Irish businesses over €2 billion in 2020 alone". In my opinion, cybercrime isn't regarded as a major worry for small businesses in Ireland, even though they are using some form of electronic communication to store customer details, they feel they won't be susceptible to a cyber-attack. Nowadays most monetary transactions are paid electronically; therefore, IT security should go hand in hand with a POS system. ERM also states that "If your company uses IT systems to conduct business, to store sensitive customer data (e.g., names, addresses or banking information), or to process card payment information, then you should consider cyber insurance to be a necessity." Eventually businesses of all sizes will obtain cyber insurance of some sort, as the statistics are always rising according to Hiscox Cyber readiness report there was a 10% increase in cyber-attacks in Ireland. The report also states that there was 5% uptake in cyber insurance in the same period.

5.1 How cyber-Insurance can improve aspects of a business.

Cyber insurance gives businesses a peace of mind or assurance that in the event of an attacks that they will be able to recover financially from an incident. Mitigating and managing risk factors are highly important to securing a business, its turnover and assuring a level of security for customers. According to (Parise, 2023), your insurance policy will cover the cost of acquiring professionals to help recover your systems. With the continuously rising number of cyber-attacks, having cyber insurance will soon be a requirement of the customer, third parties, and service providers.

6 Current Cyber Insurance practises in Ireland

From my research, most cyber insurance providers don't disclose to a member of the public how exactly they perform a risk analysis on a potential customer, after speaking with consultants in the industry. I was informed that insurance applications in Ireland are basic, with a relatively small number of questions asked, and usually given to the potential customer as a paper-based application or an Excel sheet.

6.1 Cyber Insurance Applications Worldwide

I found it difficult to find an insurance application that was created for Irish customers however, I did find insurance applications from American organisations that have given me insight as to the types of questions asked. These applications are provided by USLI and AIG-USA. There are questions that are taken from some frameworks like my own idea. The applications can be reached here: USLI Application & AIG Application.

Both applications are tick boxes for the user to provide input for certain questions, with open boxes to allow for written sections. The AIG application is difficult to navigate through and it has some controls that have stars to show significance in the application. The USLI application is not as complex as the AIG application.

6.1.1 USLI Application Screenshots

Type(s) of personally identifiable information collected, transmitted, or stored	Number of records collected or transmitted per year	Maximum number of records stored at any one time
Social security number or individual taxpayer identification number		
Financial account record (e.g. bank accounts)		
Payment card data (e.g. credit or debit cards)		
Driver's license number, passport number or other state or federal identification number		
Protected health information (e.g. medical records)		
Username/email address, in combination with password or security question		
Other – Please provide details		

Fig 5: USLI text boxes for number of data records stored.

IV. WEBSITE MEDIA LIABILITY

7. Does the applicant have a website or utilize a social media platform?	❑ Yes	❑ No
If "Yes," please answer the following regarding the content used online:		
a. Does the applicant review material that is posted or utilized online?	❑ Yes	❑ No
b. Does the applicant obtain written releases from all images used?	❑ Yes	❑ No
c. Does the website have a privacy policy?	❑ Yes	❑ No

V. SECURITY MEASURES

Information/Network Security Risk Management

8. Does the applicant utilize the following controls?		
a. Anti-virus/Malware protection on all internet accessible devices	❑ Yes	❑ No
b. Firewalls or service that has configuration-designed and maintained to protect data	❑ Yes	❑ No
c. Intrusion detection software or service	❑ Yes	❑ No
d. Passwords that are complex and contain at least eight characters	❑ Yes	❑ No
e. Passwords that are changed every 90 days	❑ Yes	❑ No
f. Have an updated system that utilizes chip card technology	❑ Yes	❑ No
g. Default passwords changed on all third party hardware and software products	❑ Yes	❑ No
9. Does the applicant proactively address system vulnerabilities, including regular updates to anti-virus/ malware protection and critical security patches?	❑ Yes	❑ No
10. Has the applicant had a vulnerability assessment, penetration test, or other network security assessment performed in the last 12 months?	❑ Yes	❑ No
11. Does the applicant have a data retention and destruction plan in place that includes both electronic and physical data?	❑ Yes	❑ No

Information/Network Security Policy

12. Does the applicant have a written physical and network security policy in place?	❑ Yes	❑ No
13. Do all employees receive training on the privacy policy at least annually?	❑ Yes	❑ No
14. Does the applicant have a designated individual responsible for the management of, and compliance with the applicant's security policies?	❑ Yes	❑ No
If "Yes," what is the name and title of this individual? _____		

Fig 6: Questions that are likely taken from certain Frameworks.

7 Use cases showing the repercussions of not having cyber insurance.

7.1 BitPay

In 2014 BitPay were hacked through their CFO, and an email was sent to their CFO Bryan Krohn, according to (Ragan, 2015), almost 5000 bitcoin were stolen "with a value of 1.85m". BitPay filed a claim for their maximum cover, however, due to the policy they purchased, the insurance company did not have to pay. Cyber policies must be carefully read before signing off, and due to the type of attack, they may as well have no insurance, costing them in full $1.85m.

7.2 Total Recall Info. Mgmt. v. Federal Ins. Co

Total recall lost computer tapes out of the back of a truck which contained sensitive info. The tapes were lost and $6m was spent to try and recover them. The company tried to claim the amount t back under general liability. According to (Chesler & Yousef, 2016) Although the tapes were lost, information was never published which left Recall with the cost of the

incident. Insurance is important, furthermore, having the correct insurance suitable for your company is paramount.

8 Scoring system

The purpose of the scoring system would be to give both the client and the third-party vendor a detailed indication of how secure their infrastructure is both positively and negatively.

The marking system would be out of a number e.g., 1000 and for each control in place the third party would receive 10 points. For each control they have not in place, the result will be negatively marked. The reason they would be negatively marked is they should have these controls in place to have a good security posture and failing to have them is a greater risk for the insurance company. In certain areas of the business, such as the physical layout of equipment or hardware there would be several questions regarding their readiness for an incident. With a good security posture, the customer would naturally score well in this field. With questions such as:

- Does your system use a DMZ network?
- Is your edge router using the latest stable software version?
- Do you ensure remote access is only available when on a secure connection (VPN etc)?

Once a score has been generated for the potential customer, the insurance company can then discuss and decide whether the potential customer is under their risk threshold. Originally, I felt that the idea would be to point out areas where the customer may lack security in certain areas and give them the chance to implement controls to further increase their score allowing them to gain bigger clients. However, as I thought more about this, the insurance company should not provide feedback for the customer as it is not a priority of theirs. It is up to the potential customer to have the necessary controls in place to situate its company under the insurance company's risk threshold.

Originally, I felt that the scoring system would vary from business to business as there may not be a need for such a high score for a small business' data for various reasons such as manpower or financial ability to further secure different areas. A smaller business might not be dealing with a huge amount of data or new technologies whereas larger enterprises cannot allocate enough of a budget each year on security as there are constantly evolving incidents/attacks e.g., power shortages in data centres. Economies are currently finding it difficult to fulfil the amount of power that is being consumed daily, which affects availability.

Businesses such as AWS would need to hold a very high score as they provide cloud computing services which would need to be protected substantially as they are dealing with millions of businesses each day. Therefore, their insurance premium would be quoted accordingly, considering the Standards they adhere to.

8.1.1 Creating/Obtaining a scoring system.

In my research, I have found that companies are using an assessment that has been created internally and using their own scoring system. It is particularly hard for me to obtain the actual scoring system that they are using.

SIG (Standardized Information Gathering Questionnaire) allows businesses to tailor questions for their company's needs however, I am looking to create an application for all vendors to adhere to. Which gives the same total score for each assessment and therefore which keeps all assessments accurate.

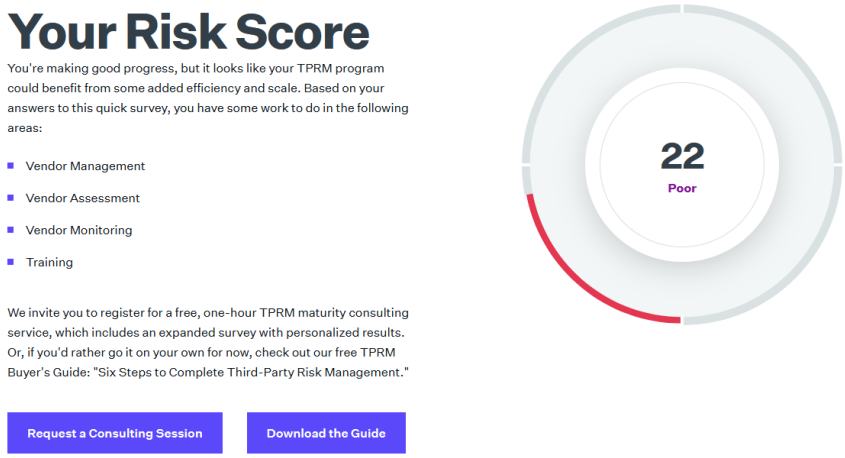


Fig 7: Risk score obtained from (Prevalent, 2023)

I obtained a template of a vendor risk assessment which is a benefit to my research however, it is a broad risk assessment where it barely scratches the surface of IT security which I will investigate further. Their scoring system is 1-5, 1 being of low importance and 5 being critical. I presume it scores as they want to, keeping their scoring system to themselves. The vendor risk assessment is prior to the change of project.

Commented [CS2]: the figure above needs a number (fig x), a caption, and needs to be referred to from the text :-)

8.1.1.1 NIST CRS

There is a similar scoring application used by NIST – the CRS (Cyber Risk Scoring). Similar to my idea, providing an application to the client and then determining and applying controls. There are similarities however, my questionnaire is solely based on the IT Security where each company will complete the same questionnaire to establish a score for their company which determines if their risk is too high to insure. The NIST scoring system (2021) uses "a weighting stated 1-10 based in an analysis of its importance to the security and privacy posture".

8.1.2 Implementing my own scoring system

During my research I have realised that for any company using an assessment like my idea, they withhold the information regarding the actual scoring system they have in place. I had my suspicions that this would be the case from the get-go. My goal is to create a self-developed scoring system with certain questions leading to a detailed insight into the IT posture of the client's business. To calculate the severity of each question in each section I will create a risk matrix to create an accurate appraisal of the client's posture.

8.1.2.1 Possible Application scoring

The scoring system can be weighted in two different options, one being a points system for example 10 for yes 5 for partial and 0 for no controls. This would be extremely accurate and leave the client with an exact result of the application. The other option would be to create a percentage result. This option wouldn't be as accurate however, it would allow businesses who just qualify for a certain mark, e.g., gaining a B mark by just making the score line. However, it would not benefit the vendor as it does not give an exact representation of the client's security posture. For the application, each question or control for the vendor to answer would have four possible answers. Each answer has will result in different weighting reflecting to the final score.

1.Yes, this control is in place/Policy implemented

2.Control/Policy is partially in place

3. Control/Policy is not in place

4. Not applicable to the vendor

If the potential customer has not got a certain policy/control in place or they feel that a certain question is not applicable to them, it would demonstrate a gap in their infrastructure. Missing a policy/control may jeopardise their business by having a weakness in that threat actors may exploit, which may lead to a breach.

9 Risk management & Compliance

Risk management is in place to prevent damage to a client's assets etc, compliance is controls, laws etc that are put in place to ensure a company follows them to protect their assets and their third parties as stated by (Agrawal et al., 2014) "compliance activities ensure that your organization's conduct does not put investors and other organizations at risk".

9.1.1.1 Risk Assessment

The purpose of a risk assessment is to identify risks that are associated with the business and evaluate the severity of those risks. There are two main types of risks: Qualitative and Quantitative. Quantitative assessment measures risk using monetary amounts whereas Qualitative uses a risk matrix to determine the likelihood and the severity of an incident. Risk Identification, risk analysis and risk evaluation are the three basic processes of a risk assessment.

9.1.1.2 Risk Identification

Identifying and creating a list of assets varying from data to finances. Once the assets have been identified, place them in order of severity i.e., assets your business cannot function without, to assets that may cause minor disruption. After identifying the assets, threats need to be identified also. In this case there is no need to identify them as the application is to check the IT posture.

9.1.1.3 Risk analysis

Risk analysis helps to evaluate the factors of each risk scenario, to identify the impact of a risk happening and the likelihood of the risk occurring. The likelihood of it happening has the following factors according to (Cyber Security Agency of Singapore, 2021), Discoverability, exploitability, and reproducibility. Discoverability being how easy a vulnerability would be to exploit. Exploitability being how the attacker would exploit the vulnerability and reproducibility; how an attacker could reproduce the attack on a vulnerability. Using this, depending on the input from the user, the application will be able to determine how severe and/or likely the business is to suffer a breach. If the client has several high chances of an incident with physical vulnerabilities, the application will flag a critical problem that needs to be addressed to the user and advise what areas to strengthen. The application will only be as accurate as the user's data. Therefore, it's in the user's best interest to answer accurately. An applicant's failure to provide accurate information will hinder them when trying to claim for an incident.

9.1.1.4 Risk Evaluation

As stated by (Ross et al., 2016) the "Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable". Clients can decide whether a risk needs a policy/control etc., implemented to reduce and or mitigate the risk of an incident or to deem a risk tolerable. E.g., Not having hurricane insurance added to your policy as it would be extremely rare to occur in Ireland.

Likelihood Rating	Discoverability	Exploitability	Reproducibility
Highly Likely (5)	The vulnerability of the target: • can be discovered by searching / scanning the public domain for published information (e.g. Shodan, ExploitDB); • can be discovered and attacked from external networks (including the internet)	The attack: • can be performed with no access rights of the target; • can be performed with publicly available tools without technical knowledge	The attack: • can be repeated at will without any specific configuration[10] or event condition[11] • can be repeated at will without any customisation of the published exploits
Likely (4)	The vulnerability of the target: • can be discovered by probing the target (e.g. port scans); • can be discovered and attacked from adjacent subnets or network segments	The attack: • can be performed with restricted access rights of the target (e.g. user); • can be performed with publicly available tools with basic technical knowledge	The attack: • can be repeated given certain configuration in the target • can be repeated with minimal customisation of the published exploits (e.g. change of parameters)
Possible (3)	The vulnerability of the target: • can be discovered by examining the target's responses, behaviour and communications (e.g. fuzzing with network packets, network sniffing); • can be discovered and attacked from within the same subnet or network segment	The attack: • can be performed with privilege access rights of the target (e.g. admin/SYSTEM/root) • can be performed with publicly available tools that requires moderate technical knowledge	The attack: • can be repeated given certain predictable event condition • can be repeated with customisation specific for the target
Unlikely (2)	The vulnerability of the target: • can be discovered by operating and interacting with the	The attack: • can be performed with privilege access rights (e.g. admin/SYSTEM/root);	The attack: • can be repeated given certain random event condition

Likelihood Rating	Discoverability	Exploitability	Reproducibility
	actual or similar setup of the target; • can be discovered and attacked with logical local access	• can be performed with publicly available/specialise tools that requires advance technical knowledge • may requires chaining of multiple exploits	• can be repeated theoretically or with published proof of concept exploit
Rare (1)	The vulnerability of the target: • can be discovered by studying the blueprint (e.g. source code) • can be discovered and attacked with physical access	The attack: • can be performed with privileged access rights (e.g. admin/root/SYSTEM) and required multi-factor authentication; • can be performed with specialised tools that requires expert technical knowledge • requires chaining of multiple exploits	The attack: • cannot be reproduced on the target • can be repeated with unpublished exploit specific for the target

Fig 8: Assessment explanation of likelihood. (CSA, 2021)

9.1.1.5 Risk Tolerance

With any business there must be a threshold as to what actions are required for different scenarios. This being from something small to a critical incident which may compromise the company. This will determine what risk the company is willing to allow in any incident, see figure below.

Risk Level	Risk Tolerance Description
Very High	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.
High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month.
Medium High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.
Medium	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.
Low	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.

Fig 9: Risk Tolerance scale (CSA, 2021)

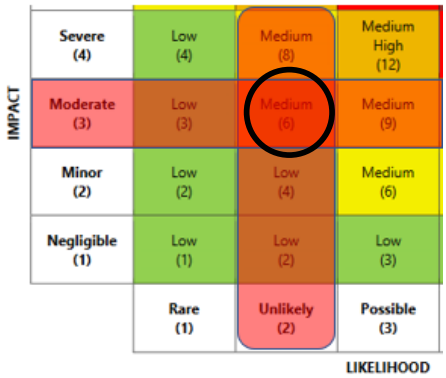
After identifying, analysing, and understanding the tolerance of a risk. A Risk Matrix is used to determine the criticality of an incident and assign it its severity based on the impact and the likelihood of it occurring.

To determine the criticality of an event, using the DRED risk matrix will determine the outcome of a possible incident or threat.

Taking the small business' edge router for example. Is the router visible to anyone? The likelihood of a threat actor accessing it is rare to unlikely, however if they do gain access to the network, they could do significant damage to the network and its systems. Using the risk matrix (see figure below) it can be calculated that it would be a medium risk. Despite being highly unlikely, it has the potential of seriously harming the business.

IMPACT						
	Very Severe (5)	Medium (5)	Medium High (10)	High (15)	Very High (20)	Very High (25)
	Severe (4)	Low (4)	Medium (8)	Medium High (12)	High (16)	Very High (20)
	Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium High (12)	High (15)
	Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium High (10)
	Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
		Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Highly Likely (5)**
				LIKELIHOOD		

Fig 10: Risk Matrix (CSA, 2021)



Adapted Fig 11: Risk Matrix

9.2 Risk Methodology

Along with the risk matrices, calculating the risk can be done using the following:

Strategic importance x Asset Importance x Likelihood = Risk Score

Strategic Importance of the asset	1 – 5
Vulnerability	1 – 5
Likelihood	1 – 5

The risk would be a 5, the vulnerability would be a 4- 5 (take 5 as it's the higher level), and the likelihood would be a 4.

Risk score	Severity
1 -42	LOW
43 -84	MEDIUM
85 -125	HIGH

Assessing the risk

Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

With this Risk assessed at 100 out of a possible 125, it is deemed severe.

9.3 Assessing Risk

9.3.1 Correlation of Risk weight and Strategic Importance

Strategic Importance of 1 is a risk weight of 1 or 2.

Strategic Importance of 2 is a risk weight of 3 or 4.

Strategic Importance of 3 is a risk weight of 5 or 6.

Strategic Importance of 4 is a risk weight of 7 or 8.

Strategic Importance of 5 is a risk weight of 9 or 10.

9.3.2 Likelihood

1-Threat is expected to occur outside 3-year window

2- Threat is expected to occur between 3 years and 2 years

3- Threat is expected to occur between 2 years and 1 year

4- Threat is expected to occur between 1 year and three months

5- Threat is expected to occur within a three-month window

9.4 Frameworks Suitable for the Application

There are multiple areas of the Vendor's IT posture to investigate and use questions from each of the suitable frameworks. Using NIST and ISO 27001 & 27002, etc. There are several controls that are applicable from different frameworks in different sections especially compliance. If the vendor has implemented compliance controls, it will increase its posture. There are multiple controls that are similar to different frameworks, such as control GV.PO-P5 from the NIST Privacy Framework and the compliance control 18.1.1 from the ISO 27002 Framework. The control would determine whether the vendor is implementing the contractual, regulatory, and statutory controls.

This control is crucial to meet as it will increase the vendor's reputation when it comes to certification and future business with third parties.

ISO 27002 control 15.1.1 addresses the security requirements for mitigating risks with a supplier's access to the vendor's assets, and it should be agreed upon. This control breaks down into smaller controls such as "c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;". Also, this is similar to GV.PO-P5 from the NIST Privacy Framework.

There are multiple frameworks that are suitable for the application, however at present I think taking controls from a variety may serve a better purpose and generate a detailed representation of the Vendor's IT posture.

9.4.1 Types of Questions

Questions should include all aspects of the IT security Infrastructure. They would include: The physical aspect of the vendor, policies implemented, standards being followed, procedures etc risk policies? Their product? Their third-party vendors. When the third party answers each section, it will produce a detailed picture of their current IT posture. Each section would then be broken up into a series of questions that would lead to a perfect section in a perfect world. Usually, it would only be the larger companies such as AWS that would be regarded as secure as they have a never-ending budget/resources at their disposal.

Questions that I may use may come from various sources, those being from gaining knowledge in general from my course whether it being a router is not accessible to unauthorised users I learned in

networking, or whether the company is following aspects of GDPR when dealing with user data information which I obtained from my legislation module. Also, there are other questions that I will gain from outside sources such as NIST or ISO 27000 series, friends, other companies, websites etc.

9.4.1.1 Physical Questions

Sample questions that may be included in the questionnaire.

Is your edge router visible to the naked eye (router)?

Is there a designated locked room for your network and storage?

What edge router defence are you using? DMZ, multi-layer approach or single edge router?

(Are you using a single router which is acting as firewall etc?)

Is there restricted access to these rooms?

Has the room a UPS (Uninterrupted Power Supply)? Can it deal with fire?

Is confidential data destroyed e.g., data written on paper?

9.4.1.2 Policies Questions

Do you backup your data?

If yes, where do your backups reside?

- On-site
- Off-site
- Off-site and cloud

Is there an information security policy?

How is user data protected? CIA (Confidentiality, Integrity, and Availability) – GDPR?

Adequate training for employees who are dealing with user data etc?

Is AAA implemented?

- Do users have authorisation?
- Is there authentication?
- Are users being accounted for?

Is the vendor providing customer support?

Do their visitors, contractors etc abide by their policies, procedures etc? (Signing in and receiving an induction?)

9.4.1.3 Compliance Questions

Do they comply with NIST Framework or ISO 27001 or another framework?

- If the answer is not sure, then the vendor is already vulnerable.

What Framework are they using?

Answer: NIST, ISO 27001,27002 COBIT, GDPR or other
(If the answer is Hybrid follow up with the next question.)

If a hybrid framework is being used, has it been customized to their business?

Is any data accessed outside of their network encrypted? Any authentication on viewing of data?

Are servers and software kept up to date to reliable version?

9.4.1.4 Reviewing/Monitoring Questions

Monitors any access to servers etc after work open hours?

Any old accounts or information that is of no use or inactive is deleted or removed?

Monitor the firewall/network logs weekly?

Monitoring the network by running scans daily/weekly?

Monitor failed login attempts? If exceeds a threshold, do they report?

Are you scanning the network for vulnerabilities?

(If these answers are not known etc, means there is no monitoring happening and it is vulnerable)

10 Control Research

I wish to determine how a company's security posture is valued by having the organisation complete the application and understand where the risk is in its business. Depending on the controls that are in place or are partially or non-existent, I determined the risk the insurance company takes when supplying cyber insurance. Without the application having too many questions for the customer's convenience, a list of controls is hand-picked from numerous frameworks such as NIST 800 – 53, ISO 27001, ISO 27002. Only controls with a severity of 8 and above will be included in the questionnaire. To determine how each control is rated I will carry out a Dredd risk matrix to get an accurate rating of each control.

10.1.1 URLs for Frameworks:

NIST 800 -53

ISO 27001 2013 Edition

ISO 27002 2013 Edition

10.2 Backup of Data

Does your company create backups of data regularly, such as weekly?

Protect the confidentiality, integrity, and availability of the backup – **direct from control.**

Frameworks Used - ISO 27002 – 2013 edition 12.3.1 & – NIST 800 - 53 CP-9 pg. 126

A backup policy should be in place, and it should be tested.

In the event of data loss, would it cripple the business? - possible control adds to back up?

Are you testing the integrity and reliability of the data that is stored?

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

In the event of a loss of data and there are no backups taken, it would be crippling for the organisation as it would be a loss of earnings and data.

Risk Weight = 10

10.3 Endpoint Security

Media access mp -2 ensuring access is only available to those who have authority.

Frameworks used - NIST 800 - 53 article SI-7 SI-8

The company employs verification tools to ensure that data has not been altered in any form.

similarly employs spam protection to detect unsolicited messages etc.

Is there Endpoint Security controls implemented?

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Weight = 10

Strategic Importance 1 – 5

Vulnerability 1 – 5

Likelihood 1 – 5

Strategic Importance *	Vulnerability *	Likelihood	= Risk

5	5	5	125

In the event of a breach due to a lack of endpoint security, it would cause severe damage to the organisation.

10.4 Human Controls

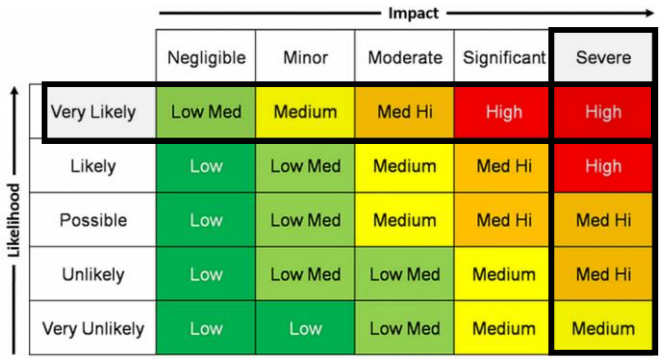
10.4.1 Agreements

Does the organisation require third-party to access systems etc., is there an agreement in place?

NDA agreements?

Agreements should address secure transfer between the organisation and third parties.

Frameworks Used - NIST 800 - 53 section PS-6 & possibly iso 27002 13.2.2



If there are no agreements between third parties, such as NDA agreements, their data, technologies etc., may be used against them intentionally or not.

Strategic Importance *	**Vulnerability ***	**Likelihood**	**= Risk**
5	5	4	100

Risk weight 9/10

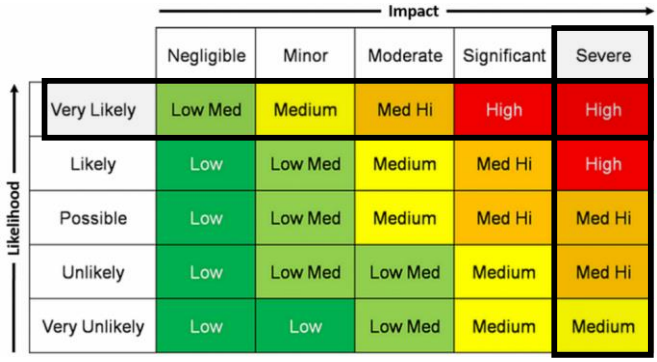
10.5 Employee access etc

Removal or termination of employee's contract

Info security responsibilities remain valid after termination or change of employment and should be defined, communicated to employees, and enforced.

Upon Employee termination, is system access revoked, and is all security-related organisational system-related property retrieved?

Frameworks Used - NIST 800 - 53 section PS-4 & possibly iso 27002 7.3.1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

It is paramount that employee access is revoked after their contract has been terminated from either party, so to ensure no information is not abused in any way, access should be withdrawn immediately.

Risk Weight = 10

10.6 Responsibilities of Employees

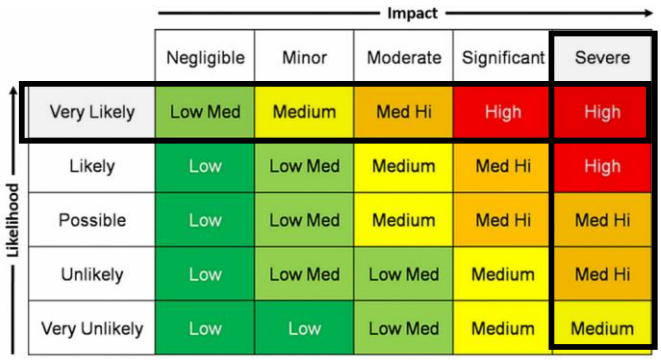
Establish a security and privacy workforce development and improvement program.

Is the company making employees aware of their cyber responsibilities through training etc.?

Development of training programs for security roles etc.

Similar controls are in place. Part c: authorisation levels should be defined and documented.

Frameworks Used - NIST 800 - 53 section PS-6 & possibly iso 27002 6.1.1



Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

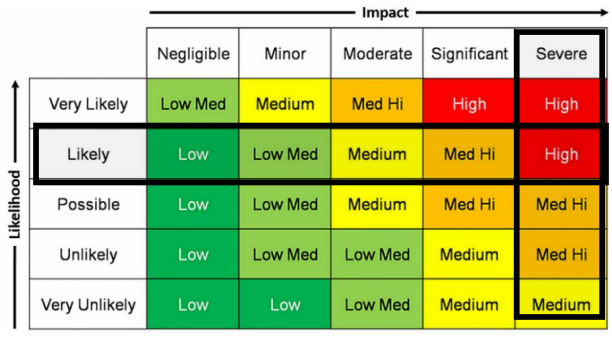
Risk weight = 9

10.7 Data Handling & Erasure

NIST 800 – 53 Revision 5 SI-13.3

Does the business take the necessary steps to destroy information that is no longer needed?

Are they destroying HDDs using a shredder etc.?



Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

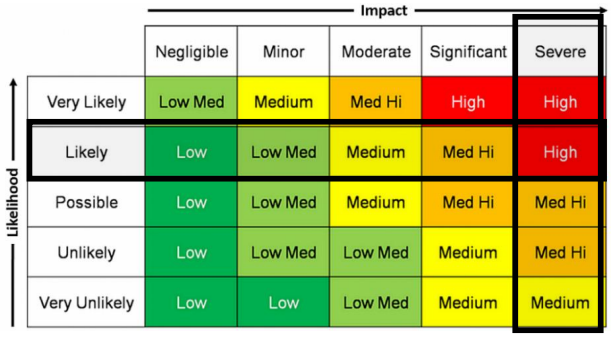
In the event of a loss of data or if it has been intercepted in some manner it would be detrimental to the organisation.

Risk Weight = 10

10.8 Data handling of file transfers

ISO/IEC 27002:2013 13.2.1 Information transfer policies and procedures

Advising employees to take necessary actions to precautions to ensure the safety of confidential data.



File transfers e.g., Ad-Hoc, can be intercepted to be viewed/modified before the recipient views the information. If files are not transferred securely, it could have devastating consequences.

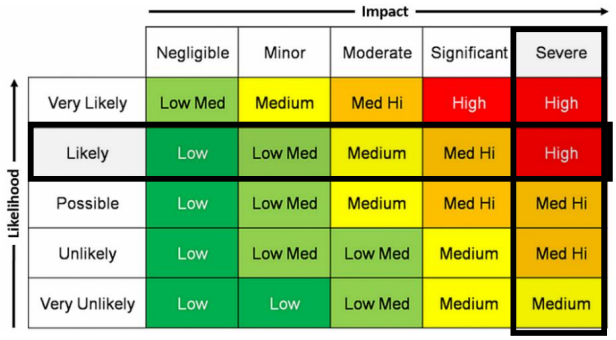
Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	4	4	64

Risk weight = 8

10.9 Media Retention

Control should be in place to ensure media is secure in a safe environment, and removable data should only be used if there is a legitimate reason.

Removable data should be limited to prevent loss of data according to IS0 27002:2013 9.3.1 (g)



Is the company monitoring all stored data, is data being recorded of deletion after removal, and is removable data disabled to unauthorised users?

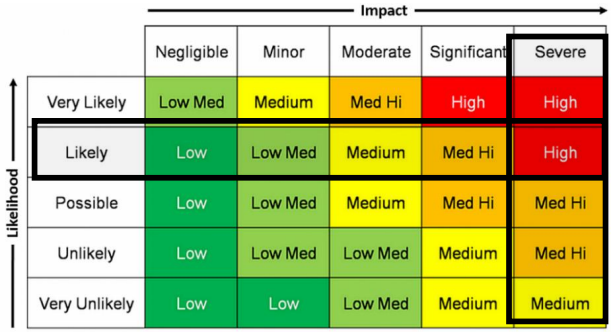
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Risk Weight = 9

10.10 Security personnel

Is there assigned personnel (Manager) that are relevant to the security of assets and information who will communicate with the board/top management?

Frameworks ISO/IEC 27001:2013 5.3 & NIST SP 800-53, REV. 5 PM-2, also PM-9



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Risk Weight = 9

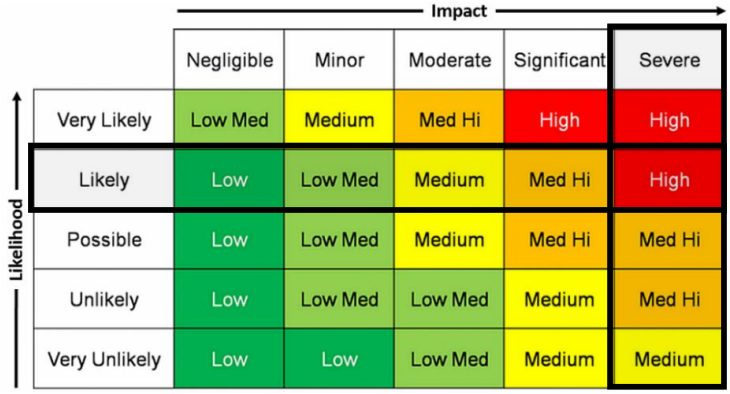
Without a security officer/manager in place, this could show negligence to security and may result in a lack of communication between management and fewer resources allocated to security.

10.11 Asset Map Management

Is there a map of where data assets are stored or transmitted? Showing how identifiable data is being stored transmitted, disposed of etc. (life cycle)

To protect the assets of the business, identifiable data should be mapped to show where data is stored and or transmitted to/from.

Frameworks NIST SP 800-53, REV. 5 CM-13



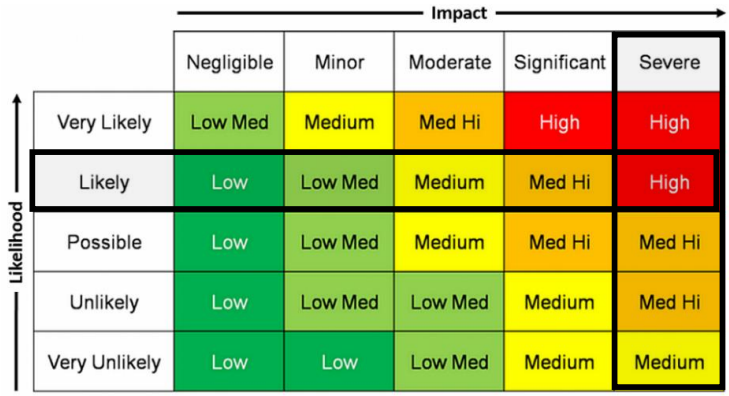
Risk Weight 8-9

Strategic Importance *	**Vulnerability ***	**Likelihood**	**= Risk**
5	5	4	100

10.12 Data Governance

Are there controls in place that ensures the organisation is following standards, and procedures and data are maintained safely?

Frameworks NIST SP 800-53, REV. 5 PM-13, PM-14



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Risk Weight = 10

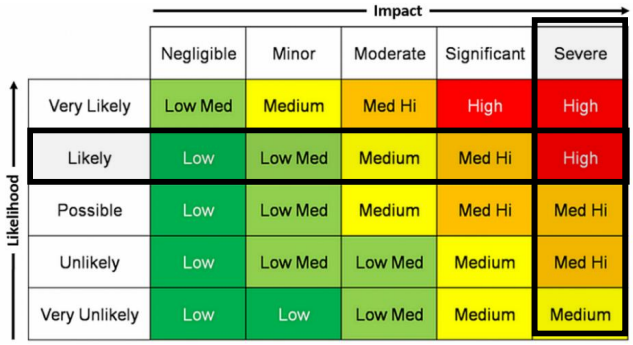
If there is no governance implemented, no standards being followed, it would leave the organisation open to vulnerabilities and it would be difficult to recover from. Third-parties or customers would have no faith in the Accountability, Integrity, and the Confidentiality of the organisation.

10.13 Asset Inventory

Is there a document etc that reflects all aspects of the organisation's system?

Such information needed to be accounted for would be System name, software owners, software version numbers, licencing components, network components, network addresses system-wide etc.

Frameworks NIST SP 800-53, REV. 5 CM-8



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

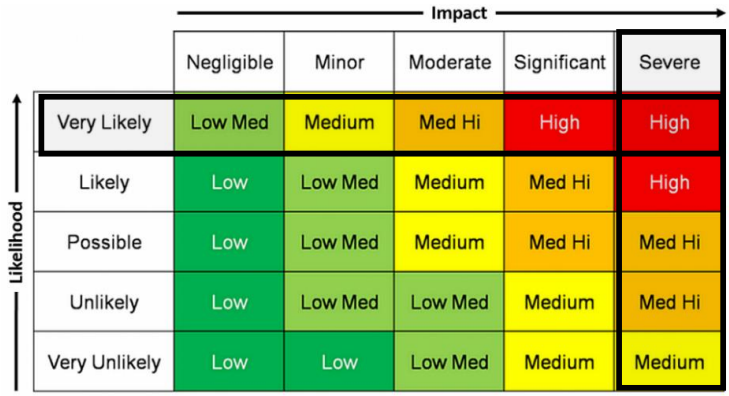
If there is no asset inventory system in place it can lead to insecure areas of the system as a piece of software may be vulnerable as it is out of date, with inventory taken it can be updated regularly and the system can be checked easily.

Risk Weight = **9**

10.14 Security and privacy plan

Has the organisation a security and privacy plan in place? Have they provided an overview of the security and privacy requirements of the system? Including the risk for certain design and security decisions? **(There are multiple controls in place in this section which can be used in the same question or dive deep in into more specific questions)**

Frameworks NIST SP 800-53, REV. 5 PL-2



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

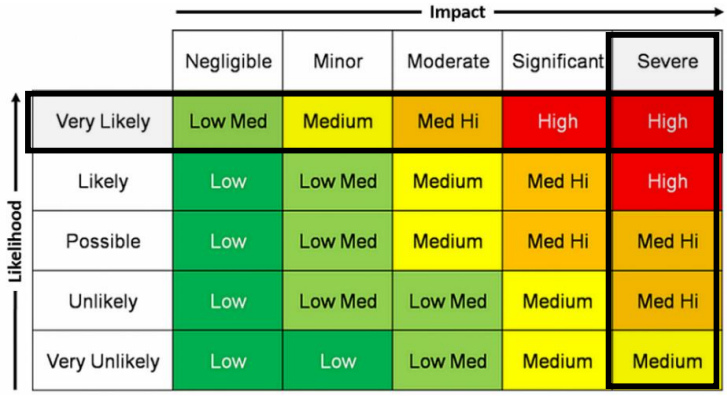
If there is no security or privacy plans in for an organisation, they would miss many areas that require attention throughout the system which an attacker may take advantage of.

Risk Weight = 10

10.15 Device Asset Management – POS etc

Are there procedures in place to protect equipment that may be left unattended, such as computers POS devices etc.?

Frameworks ISO/IEC 27002:2013 11.2.8



If a session is left open on an unprotected device it may give threat actors access to the organisations system, they may use a POS to take advantage of a victim.

Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

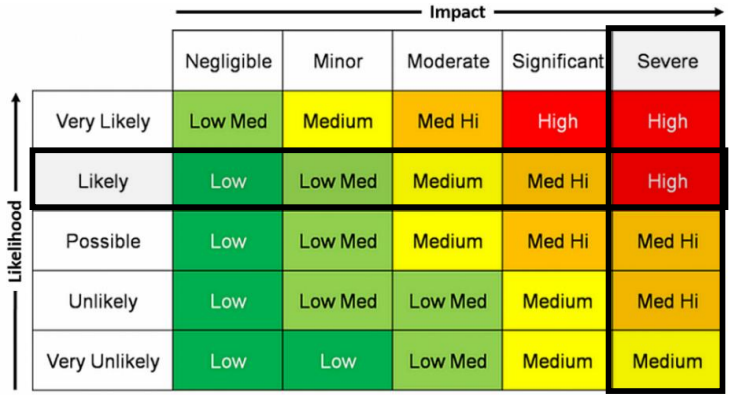
Risk Weight = 9

10.16 Offsite Asset Management

Are all off-site devices accounted for? Is there a log in place to show the chain of custody? Are there controls in place to prevent threat actors from gaining access to devices or the information on them?

Important for assets that serve a purpose for a third party, i.e. MSP devices that are returning from use in a third-party organisation.

Frameworks ISO/IEC 27002:2013 11.2.6



If there are devices that are off the organisations location it increases the chances of information being retrieved/altered on the victim device.

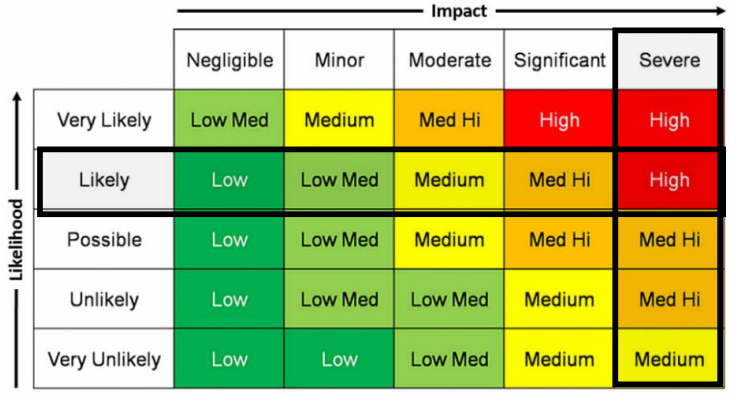
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	4	4	80

Risk Weight = 8/9

10.17 Disposal of Equipment

Devices at their end of lifetime should be disposed of adequately. Is there whole disk encryption on each hard drive that needs to be disposed of.

Frameworks ISO/IEC 27002:2013 11.2.7



Disposing of devices and Hard Drives is vital as a lot of devices are recycled by third parties and devices are re-purposed. Information can be retrieved, and sensitive information can be exposed.

Strategic Importance *	**Vulnerability ***	**Likelihood**	**= Risk**
3	4	4	48

Risk Weight = 8

10.18 Business Continuity

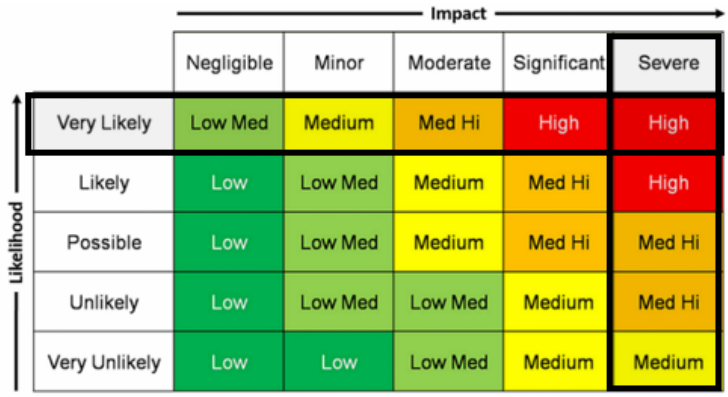
10.19 Business Continuity/Contingency Plan

Has the organisation a contingency plan in place, such as a Disaster Recovery Plan?

Is there a management in place that will be able to respond to any incidents or disasters?

Are there incident handling personnel employed?

Frameworks ISO/IEC 27002:2013 17.1.3 & NIST SP 800-53, REV. 5 CP-1, CP-2, CP-10



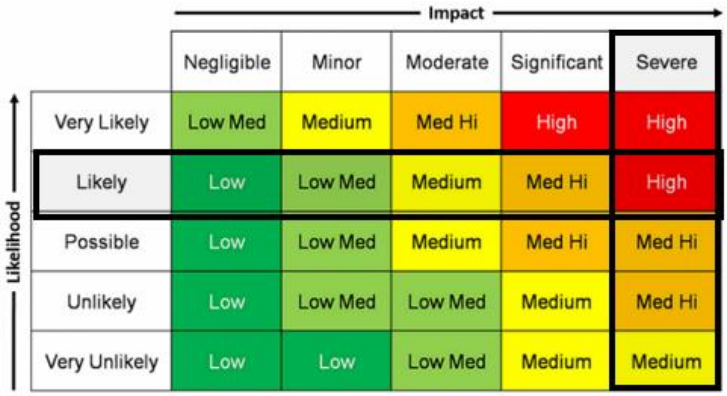
In the event of an incident or a disaster, without a contingency plan in place the organisation may not be able to recover to a prior state, leaving the organisation crippled.

Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

Risk Weight = 10

10.20 Identifying Critical Assets

Does the organisation identify critical assets to aid with a contingency plan? Has the organisation prioritized these assets so that the business can resume within a minimum time frame?



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

If there are no critical assets determined, in the event of an incident it would take an abnormal length of time for the organisation to regain productivity.

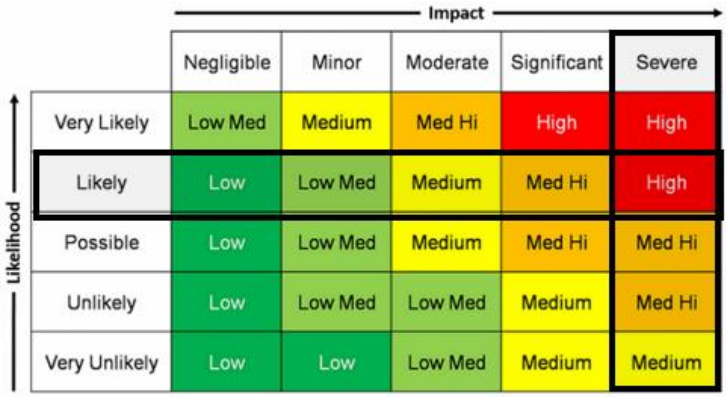
Risk Weight = 9

10.21 Root Cause Analysis/Testing

After an incident or disaster, does the organisation perform a Root Cause Analysis after the contingency plan has been implemented?

Are there SOPs (Standard Operating Procedures) in place for various tasks?

Frameworks NIST SP 800-53, REV. 5 CP-4



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

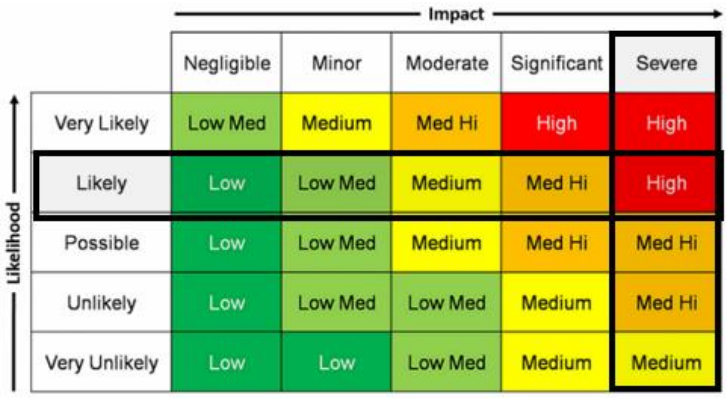
If there is no testing done when a contingency plan is in place or no testing has been carried out, when an incident occurs their response may be hindered by not carrying out the plan in detail by omitting steps unintentionally.

Risk Weight = 8/9

10.22 Alternative Security Controls

Does the organisation have other security controls in place that may not be as secure as the primary security mechanisms however, business function could resume?

Frameworks NIST SP 800-53, REV. 5 CP-13



If primary security mechanisms are unavailable an

There are no secondary available/implemented, it may cripple the business function.

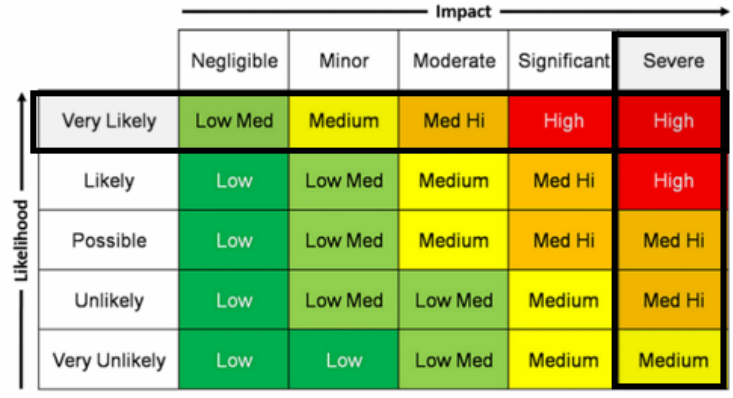
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	3	75

Risk Weight = 8

10.23 Offsite Storage

Does the organisation have an alternative storage site such as Azure?

Frameworks NIST SP 800-53, REV. 5 CP-6



If there is no alternative storage site, all data stored at the primary location may be lost in the event of an incident which would have a crippling outcome on the organisation.

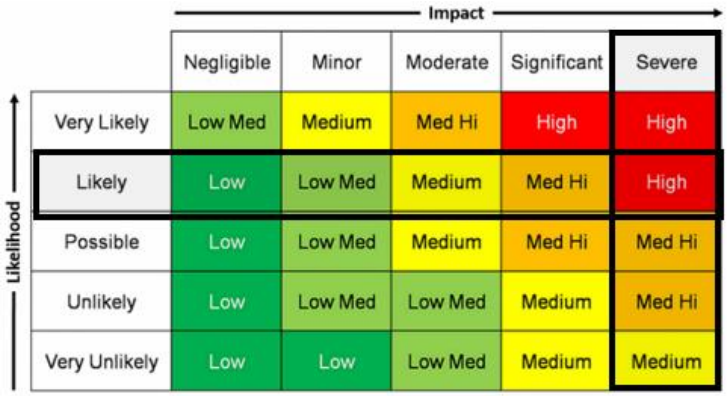
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Risk Weight = 10

10.24 Alternative processing site

Is there an alternative site to carry out all processing for the organisation in the event the primary business premises is unavailable?

Frameworks NIST SP 800-53, REV. 5 CP-6 & ISO/IEC 27002:2013 17.1.3



If the business needs physical space to use equipment etc it is important that a backup premises is available to continue processing in the event of an incident/disaster at the primary location.

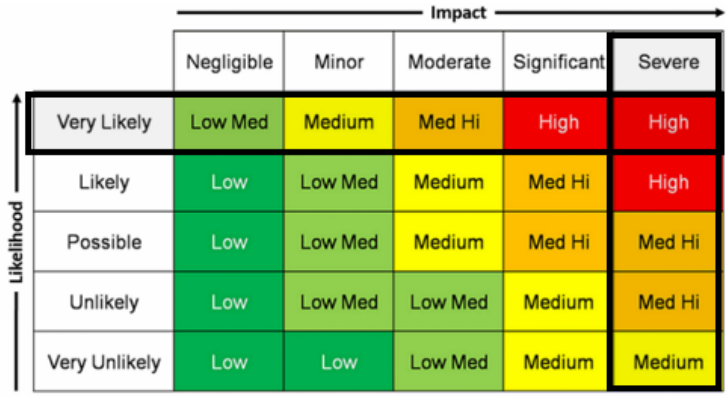
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	2	50

Risk Weight = **7**/8

10.25 System recovery

Has the organisation the ability to recover the system to a known state after an incident or failure?

Frameworks NIST SP 800-53, REV. 5 CP-10



After an incident or failure of a system it is paramount that an organisation can restore their systems back to a known state.

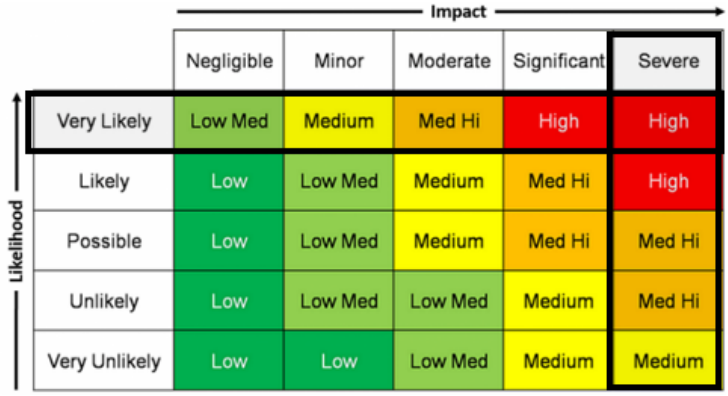
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

Risk Weight = 10

10.26 Cryptographic Backup

Is all data backed up using a cryptographic function to prevent unauthorised viewing or altering of data?

Frameworks NIST SP 800-53, REV. 5 CP-9(8) & & ISO/IEC 27002:2013 12.3.1 (f)



If data that is backed up is not stored with a cryptographic function, it may be visible for any unauthorised user to view/alter.

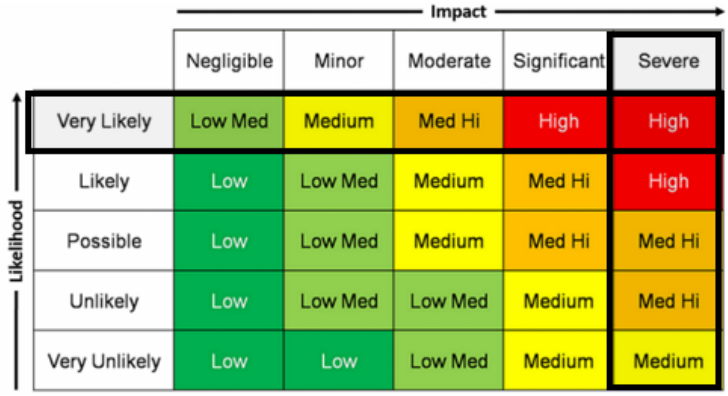
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Risk Weight = 10

10.27 Changes to Systems

Is there a control in place that any significant changes are recorded and tested before live implementation? Are there fallback procedures in place if the change needs to be aborted or configurations need to be reset?

Frameworks NIST SP 800-53, REV. 5 CM-3 & & ISO/IEC 27002:2013 12.1.2 (all subsections)



If changes are made and there is no mechanism in place to revert to a stable system, it may cause significant disruption.

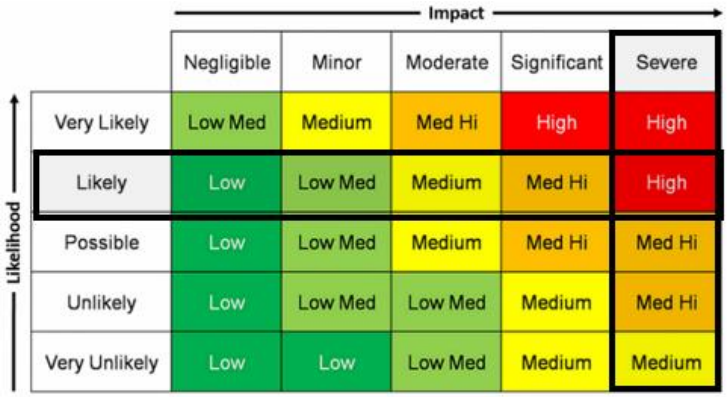
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	4	5	100

Risk Weight = 9

10.28 Unauthorised changes Control

Is there a control in place to prevent any unauthorised changes to a system? Are changes brought to top-level management to approve of changes that usually are not authorised?

Frameworks NIST SP 800-53, REV. 5 CM-3(1)



If there are no controls in place to approve changes that would normally need approval from upper management, it can lead to disorganisation and deem the system unfit for purpose.

Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	3	4	48

Risk Weight = 7

10.29 Testing of planned changes

Are business critical changes carried out in an environment and review their results prior to implementing their live system?

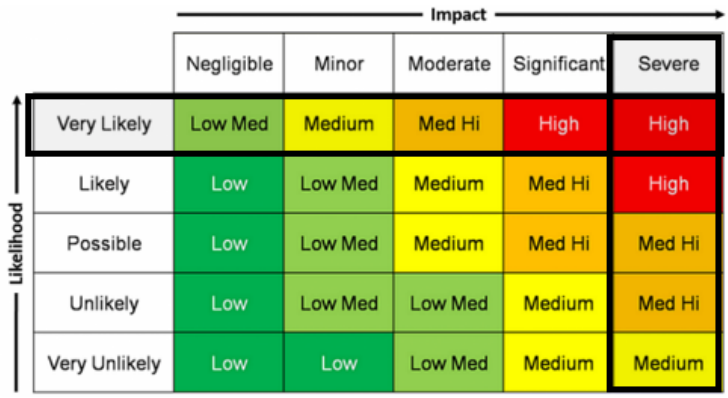
Frameworks NIST SP 800-53, REV. 5 CM-3 (2)(7) & ISO/IEC 27002:2013 14.2.3

10.30 Analysis of change impact

Does the organisation determine the potential security impacts before the live implementation of changes?

Are there risk assessments performed on changes before implementation? Will the changes affect the privacy of individuals?

Frameworks NIST SP 800-53, REV. 5 CM-4



If risk assessments are not carried out on changes it may leave the organisation susceptible to an incident, exposing assets and/or client data.

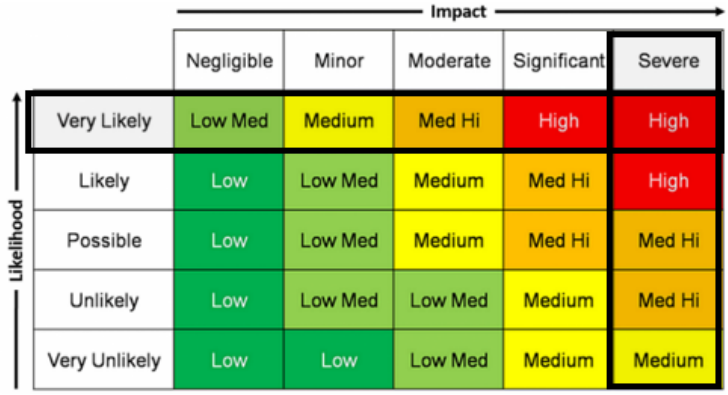
Strategic Importance *	**Vulnerability ***	**Likelihood**	**= Risk**
5	5	4	100

Risk Weight = 10

10.31 External services (cloud services etc)

If a third party is acquiring cloud services, is the third party complying with the client organisation's governance and compliance?

Frameworks NIST SP 800-53, REV. 5 SA-9



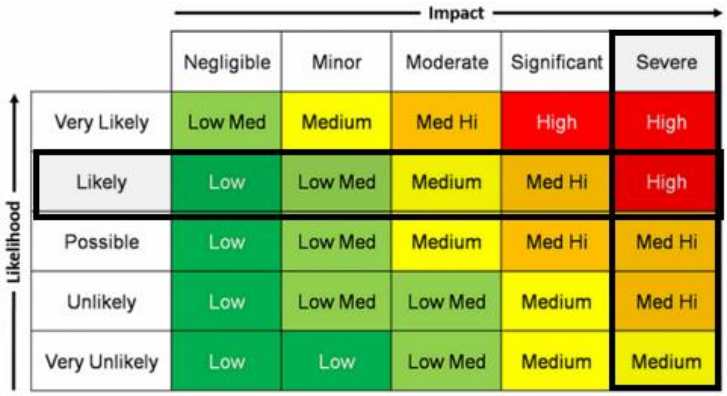
When the client is sourcing a third party, if the data they are storing is not up to theclient'ss standards or a Framework such as NIST 800 -53, they may be susceptible to a breach.

Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	3	75

Risk Weight = 9

10.32 Cloud Data Storage Location

Does the organisation have control of where the cloud services provider stores data?



To respond to an incident in a timely manner data that is stored locally can be accounted for or examined easier than the timeframe needed to get information from the third-party provider.

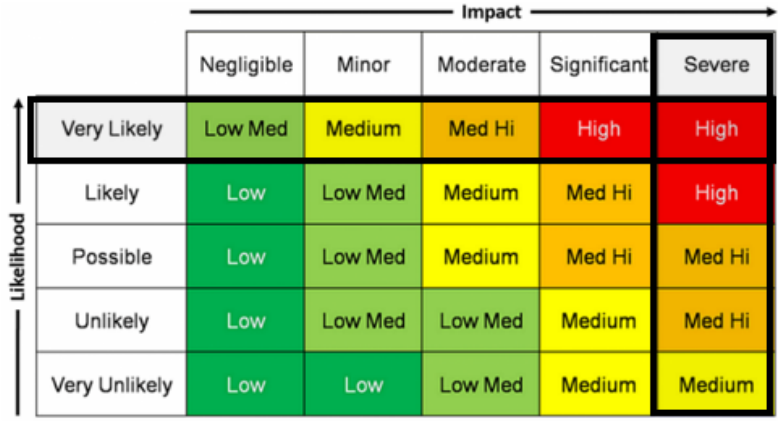
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Risk Weight = 8

10.33 Legislation and contractual requirements

Does the organisation implement the necessary statutory, and contractual controls?

Frameworks NIST SP 800-53, REV. 5 PM-8 & ISO/IEC 27002:2013 18.1.1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	2	50

It is important that organisations follow regulatory controls, and contractual obligations. Without this it fails to show competence in the company to other parties/potential clients.

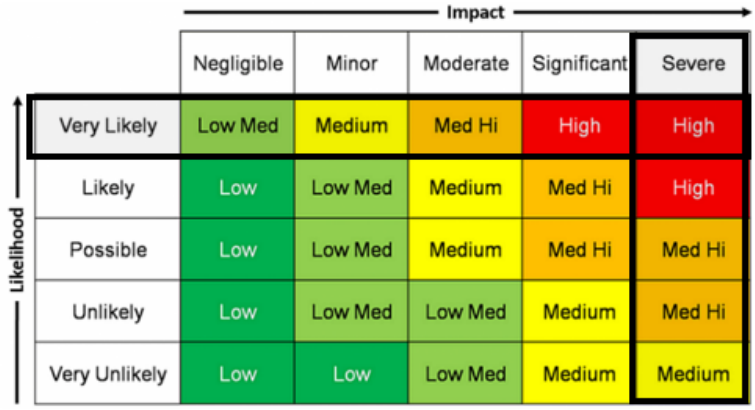
Risk Weight = 8

10.34 Executives providing oversight on controls.

Executive level review of multiple areas/decisions throughout the organisation?

Management should review continual improvement across the organisation.

Frameworks ISO/IEC 27001:2013 9.3, 10.2 & ISO/IEC 27002:2013 12.7.1



Management should be involved in any changes that may affect the system and its services, if not in can lead to poor communication preventing the organisation of running efficiently.

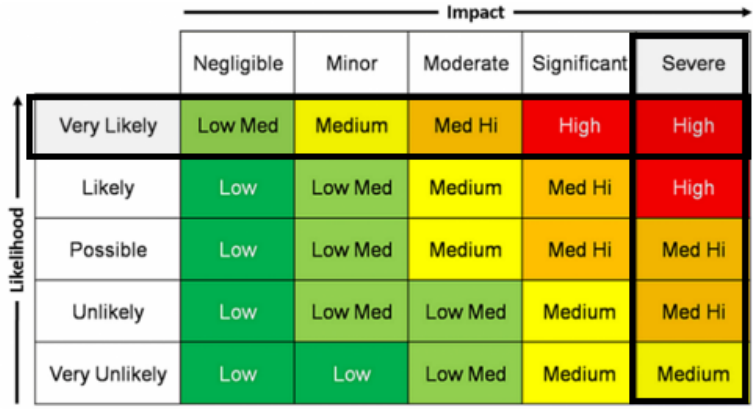
Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	3	4	60

Risk Weight = 10

10.35 Management security assessing

Is there a security manager or assessment officer in place who assesses controls and their enhancements? Are they assessing the effectiveness of a control? Who can provide an assessment report at an executive level?

Frameworks NIST SP 800-53, REV. 5 CA-2 & ISO/IEC 27002:2013 18.2.2 & ISO/IEC 27001:2013 9.2



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

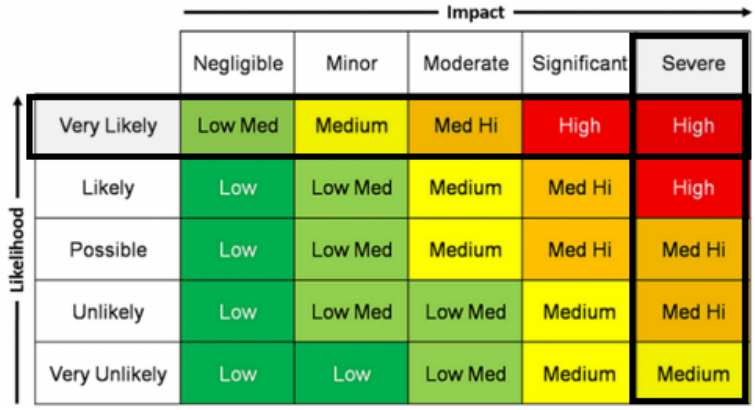
If controls and their enhancements are not being audited or assessed it may render them ineffective, particularly if enhancements to controls have not been audited and a report does not reach the executive level.

Risk Weight = 9

10.36 Baseline Setup

Is there a baseline configuration of all systems developed, documented, and maintained?

Frameworks NIST SP 800-53, REV. 5 CM-2 & ISO/IEC 27001:2013 9.1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

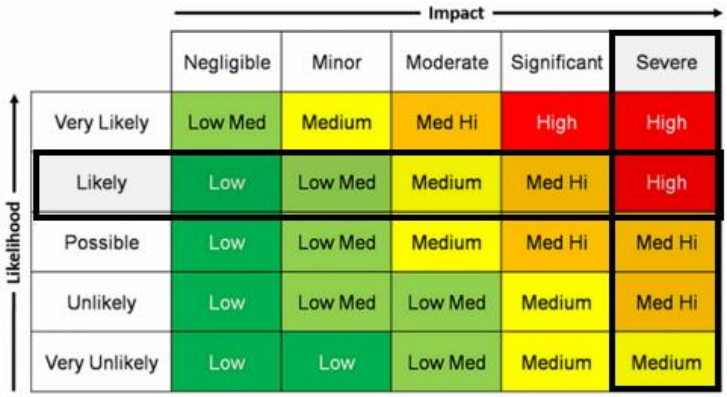
Baseline configurations are needed in the event a system needs to be restored to an earlier point. Without a documented baseline, systems may never reach a stable state again or perhaps at a much slower rate than anticipated.

Risk Weight = 10

10.37 Unauthorised access policy

If the system has altered unauthorised configurations, is it regarded as an incident?

Frameworks NIST SP 800-53, REV. 5 CM-6(2)



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	3	75

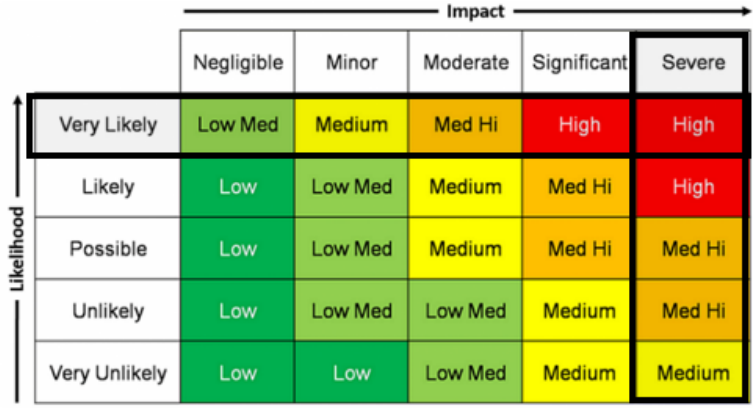
If the systems configurations have been accessed by unauthorised personnel, it may have a significant impact on the organisation as controls may be altered or removed to the benefit of a threat actor.

Risk Weight = 8

10.38 Prohibiting Capabilities/Restricting Access

Is there a control in place to reduce users' capabilities to the minimum to prevent any unauthorised changes?

Frameworks NIST SP 800-53, REV. 5 CM-7 & ISO/IEC 27002:2013 9.4.1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

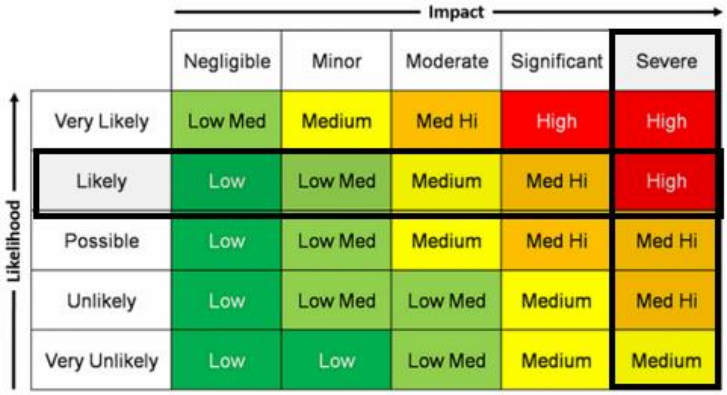
Allowing access to areas of the organisation may lead to unauthorised access which may have a detrimental outcome.

Risk weight = 9

10.39 Software Restrictions

Has the company restrictions in place to prevent the unauthorised use of software? Ensuring the use of peer-to-peer file sharing is used in line with company policies.

Frameworks NIST SP 800-53, REV. 5 CM-10



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Unauthorised use of company software or file sharing may cause the release of the organisation's data/software.

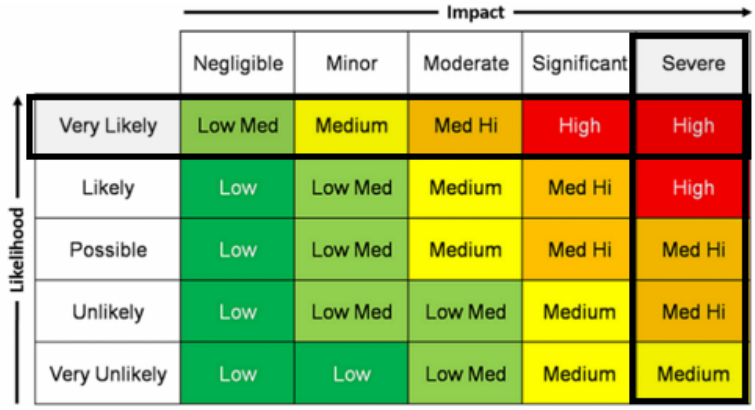
Risk weight =

10.40 Third-party Software

Has the organisation a policy in place to prevent the unauthorised installation of third-party software by an unauthorised user?

Control's another, so withdrawn from the application.

Frameworks NIST SP 800-53, REV. 5 CM-11



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

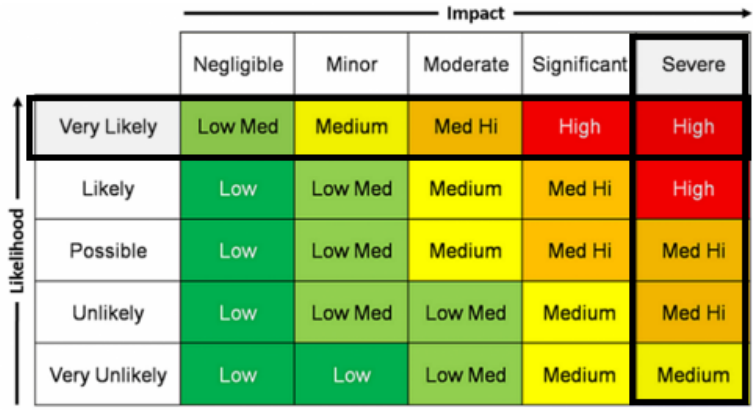
To ensure the safety of the organisation it is paramount that third party software cannot be added as it may cause unintended/intended harm to their system. Only Administrators should have the authority to add third-party software to devices from an approved list of applications.

Risk weight = 10

10.41 Event Logging

Does the organisation log all events of significance to ensure safety and record keeping of changes, such as user login and log off, timestamps etc?

Frameworks NIST SP 800-53, REV. 5 AU-2, PM-31 & ISO/IEC 27002:2013 12.4.1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

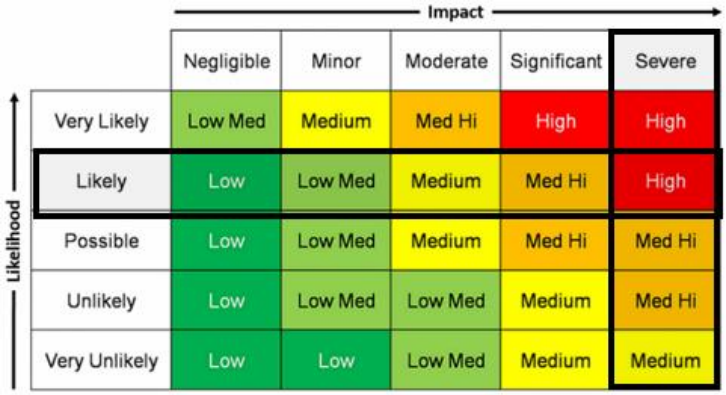
Without event logging the organisation will have no records of changes made or access granted/ denied by users etc. Events logged such as attempted log ins, remote log in attempts etc.

Risk weight = 10

10.42 Event Log Review & Escalation

Do the organisation review events that were logged and take the necessary steps in an acceptable timeframe?

Frameworks NIST SP 800-53, REV. 5 AU-2



Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	5	4	80

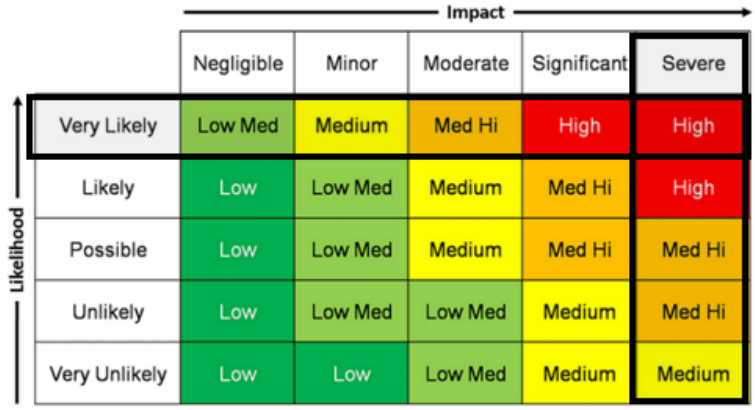
If events are logged, and there is no review or action performed, then there is no point in logging an event in the first place. Without reviewing and classifying events it makes it almost impossible to keep the system secure.

Risk Weight = 7/8

10.43 Cryptographic Protection

Does the business implement cryptographic functions using trusted cryptographic functions?

Frameworks ISO/IEC 27002:2013 10.1.1, 14.1.2 & NIST SP 800-53, REV. 5 SC-7(6), SC-8, SC-13



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

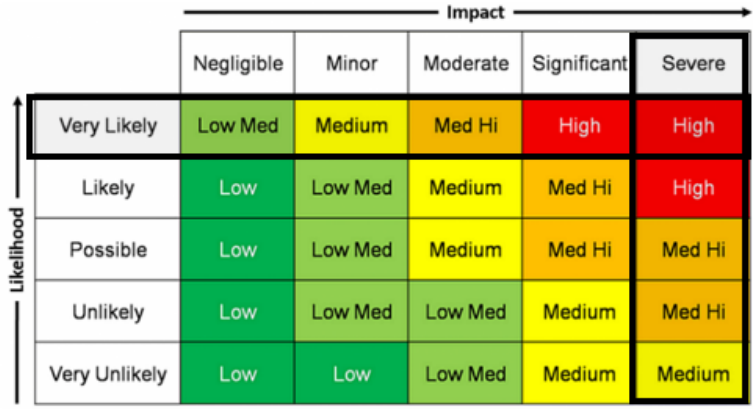
Without any cryptographic functions in place, company data would be easily accessed as all stored data would remain in plaintext, which in the event of a breach would be detrimental to the organisation.

Risk weight = 10

10.44 Cryptographic functions for data in transit

Is there a control in place to ensure data being transmitted is protected using cryptographic functions?

Frameworks ISO/IEC 27002:2013 13.2.3, 14.1.2, 14.1.3 & NIST SP 800-53, REV. 5 SC-8 SC-16(3), SC-28(1)&(3)



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

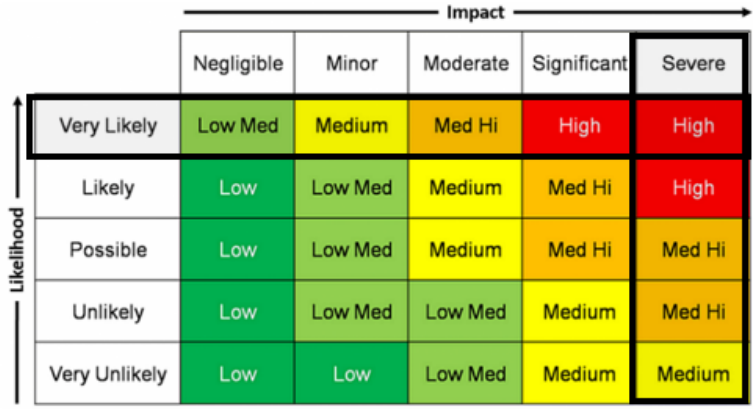
Data must not be transmitted on a network in plaintext as it can be intercepted and has no protection.

Risk Weight = 9

10.45 Data Protection Controls

Does the organisation protect data that is stored/used by the organisation?

Frameworks ISO/IEC 27002:2013 8.2.3 & NIST SP 800-53, REV. 5 MP-1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

Data protection is paramount in any organisation.

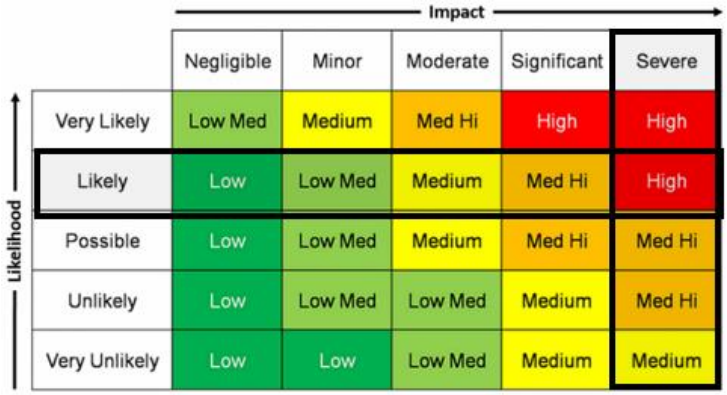
Risk Weight = 10

10.46 Media Disposal

Does the business dispose of media (HDDs etc.) when it is no longer required?

Frameworks ISO/IEC 27002:2013 8.3.2 & NIST SP 800-53, REV. 5 MP-6

Media that has not been disposed properly may leave delicate information which may be accessed to anyone who may have access to it.



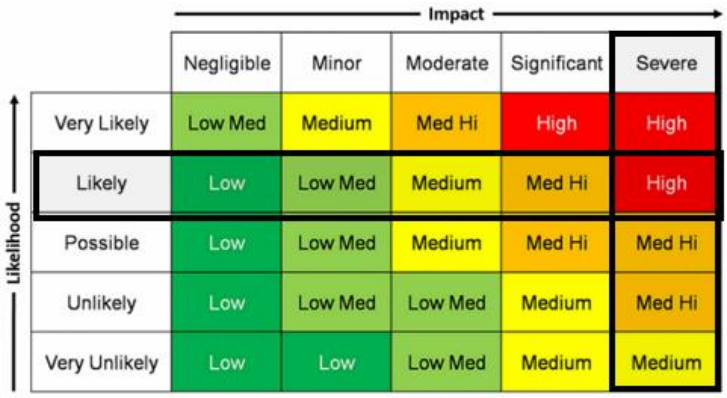
Strategic Importance *	Vulnerability *	Likelihood	= Risk
3	4	4	48

Risk weight = 7

10.47 Specific media types for systems

Does the organisation limit the types of media that can be used on specific systems?

Frameworks ISO/IEC 27002:2013 8.3.1 & NIST SP 800-53, REV. 5 MP-7



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	4	4	80

It is paramount that certain media types are restricted from operating on certain systems, such as USB access on computers.

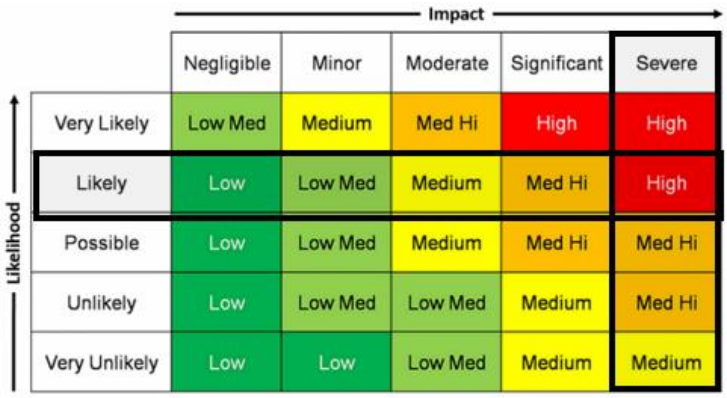
Risk weight = 8

10.48 Information Transfer

Does the organisation take the necessary steps to protect the transfer of data, ensuring that data is adequately protected?

Withdrawn from the app, as it is similar to above.

Frameworks ISO/IEC 27002:2013 13.2 & NIST SP 800-53, REV. 5 AC-21



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	4	4	80

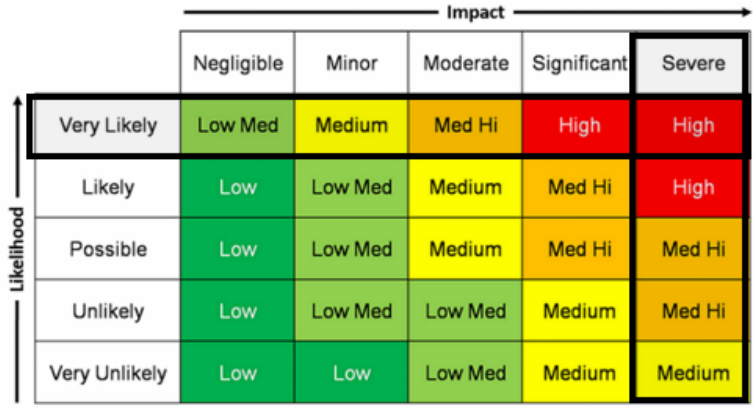
Data must be protected, and information must be protected during transfer.

Risk weight = 8

10.49 Updating of Malware Protection

Does the organisation implement a control that automatically updates malicious code protection?

Frameworks ISO/IEC 27002:2013 12.2.1 & NIST SP 800-53, REV. 5 SI-3



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

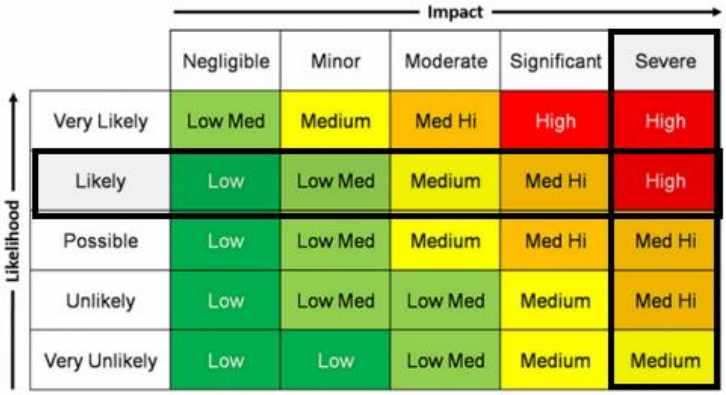
Malware protection needs to be updated regularly to help prevent an intrusion which may have devastating effects on the business continuity.

Risk weight = 8

10.50 Personnel screening

Are individuals screened before being assigned a position which comes with certain risk? E.g., background check when dealing with sensitive data?

Frameworks ISO/IEC 27002:2013 7.1.1 & NIST SP 800-53, REV. 5 PS-3



Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	4	4	64

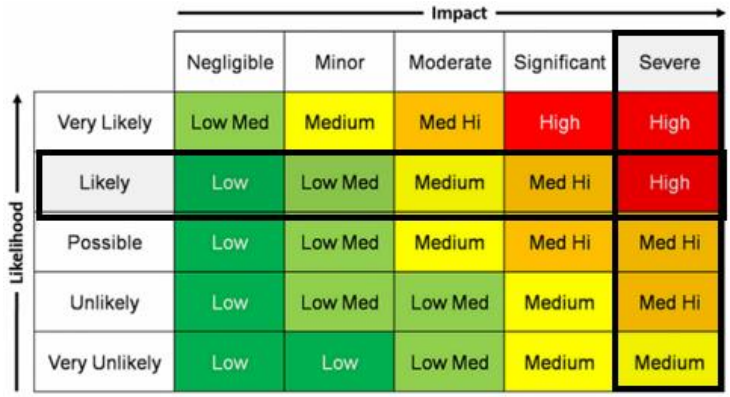
It is important to take the necessary steps to ensure that personnel would be suited for a particular role with certain risk factors involved.

Risk Weight = 8

10.51 Employment Terms and Conditions

Employees and or Contractors should sign an NDA before being given access to client confidential data. Does the company ensure that employees/third parties are responsible for client confidential data?

Frameworks ISO/IEC 27002:2013 7.1.2 & NIST SP 800-53, REV. 5 PL-4



Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	3	5	60

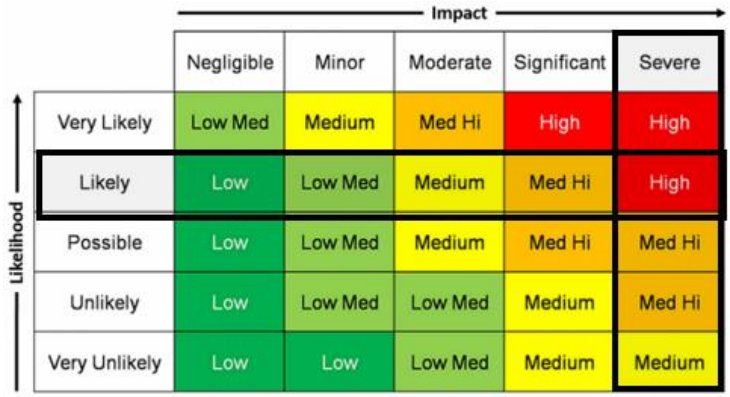
Employees should be held accountable for their actions regarding the protection of client data.

Risk weight = 8

10.52 Access agreements

Does the organisation require personnel and or third parties to sign agreements such as NDAs prior to gaining access to data?

Frameworks ISO/IEC 27002:2013 13.2.4 & NIST SP 800-53, REV. 5 PS-6



Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	5	3	60

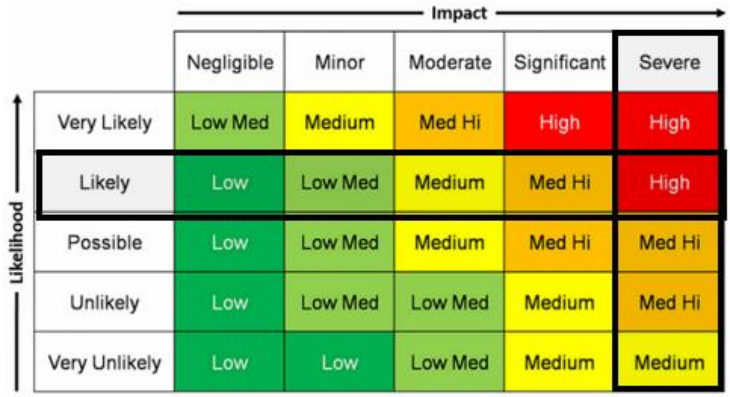
When dealing with client data by either personnel or a third-party, NDAs must be signed to ensure no information loss either intentionally or unintentionally.

Risk weight = 8

10.53 Authentication Management

Does the organisation alter default vendor authentication methods etc? Are personnel held accountable to ensure the confidentiality of authentication methods?

Frameworks ISO/IEC 27002:2013 9.2.4 & NIST SP 800-53, REV. 5 IA-5



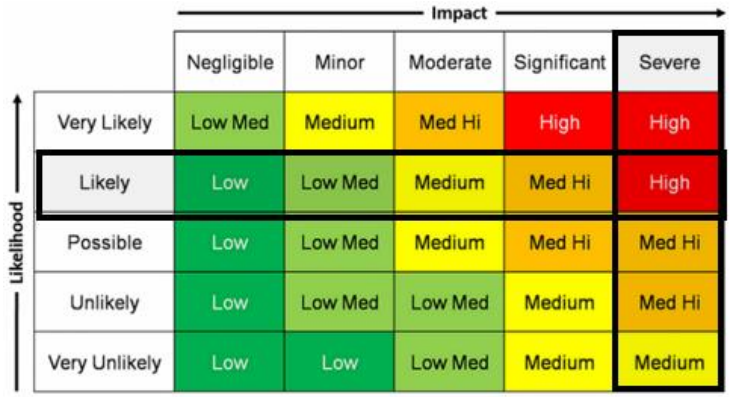
Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	5	3	60

Risk weight = 8

10.54 Password Authentication

Is your organisation implementing measures such as complexity, length, and lifespan of passwords, to ensure strong password-based authentication?

Frameworks ISO/IEC 27002:2013 9.2.4 & NIST SP 800-53, REV. 5 IA-5



Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	5	4	80

Password security is an important factor, as the complexity of the password increases, the harder it will be to compromise it.

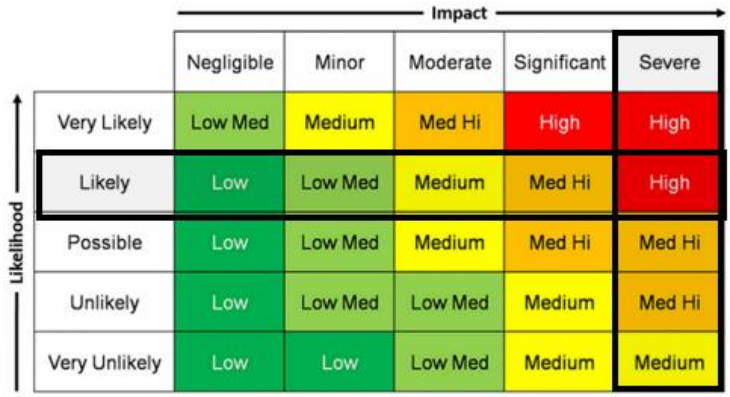
Risk weight = 7

10.55 Disable Accounts

Does the organisation use automation methods to disable accounts after a specific time?

Frameworks ISO/IEC 27002:2013 9.2.1 & NIST SP 800-53, REV. 5 AC-2

7002:2013 9.2.4 & NIST SP 800-53, REV. 5 IA-5



Strategic Importance *	Vulnerability *	Likelihood	= Risk
3	4	5	60

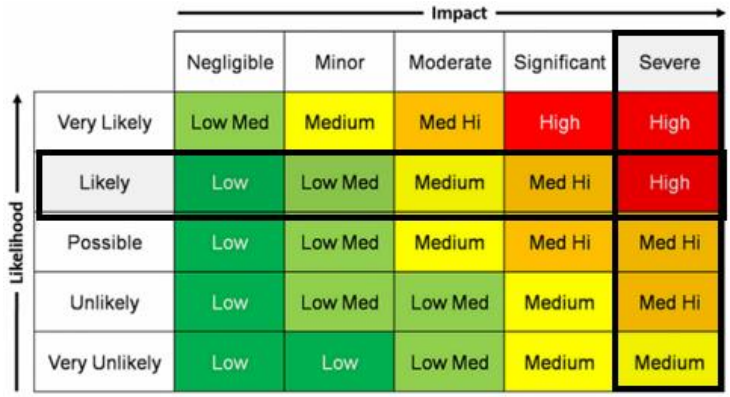
Disabling accounts is important to prevent the loss of data.

Risk weight = 6/7

10.56 Review of user privileges

Does the organisation regularly assess privileges given to users and make the necessary adjustments to give each user the least possible privilege?

Frameworks ISO/IEC 27002:2013 9.2.5-6 & NIST SP 800-53, REV. 5 AC-6



Strategic Importance *	Vulnerability *	Likelihood	= Risk
4	5	4	80

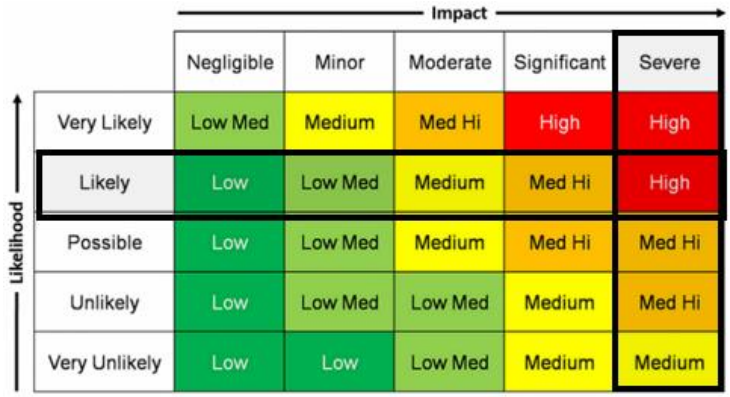
Reviewing user privileges periodically instils a good cyber security posture.

Risk weight = 7/8

10.57 Least Privilege

Does the implement the principle of least privilege, by restricting access to certain areas of the organisation?

Frameworks ISO/IEC 27002:2013 9.1.2 & NIST SP 800-53, REV. 5 AC-6 & SA-8(14)



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

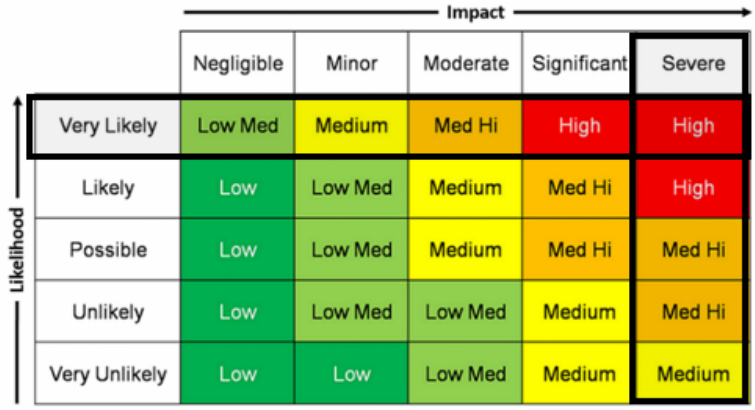
Ensuring users get the least privilege possible ensures security.

Risk weight = 9

10.58 Account Logins

Is there a policy in place that locks out the user after a certain number of attempted logins in a specific period has been reached?

Frameworks ISO/IEC 27002:2013 6.2.1 & NIST SP 800-53, REV. 5 AC-7



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	4	100

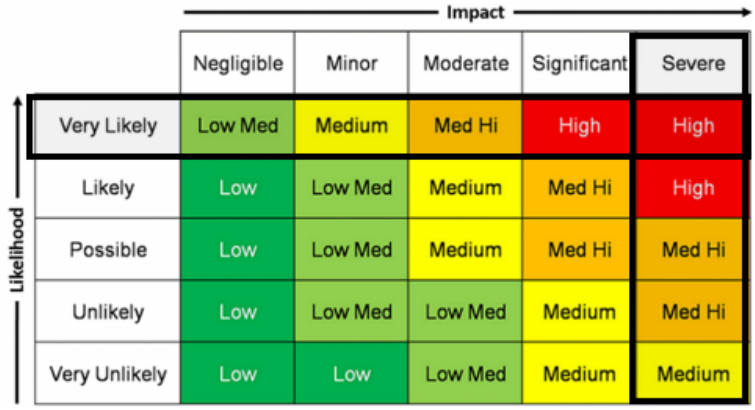
Having this control prevents brute force attacks on certain functions such as login.

Risk weight = 9

10.59 Incident Response

Does the organisation implement incident response controls?

Frameworks ISO/IEC 27002:2013 16.1.1 & NIST SP 800-53, REV. 5 IR-1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	5	5	125

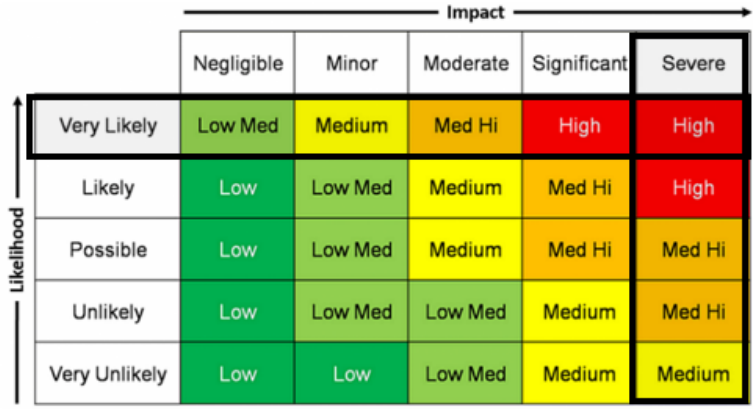
Having an incident response plan in place is vital to the survival of an organisation.

Risk weight = 10

10.60 Incident Response plan availability

Is there an up-to-date incident response plan available to all stakeholders?

Frameworks ISO/IEC 27002:2013 16.1.1 & NIST SP 800-53, REV. 5 IR-1



Strategic Importance *	Vulnerability *	Likelihood	= Risk
5	3	5	75

Having an incident response plan in place is vital to the survival of an organisation.

Risk weight = 7

11 The Application

11.1.1 Type of Application

There are two approaches suitable for this application.

One being a standalone application and the other a web app. Using a standalone app would ensure that when customers pay for the app that they have full access to its potential locally.

The other possibility would be to develop a web app. Allowing the vendor to sign in and undertake the application. After completion of the questionnaire the user's data (infrastructure score) will be stored on a database for future reference. Mobility is one of the biggest advantages of having an application nowadays with cloud computing becoming more popular each day. In turn my application would be better suited as a web app, this allows for mobility of the app. This will allow for the deployment of the application to be instantaneous as once the client has paid for the service,

they will receive their login and complete the questionnaire with no fuss or unnecessary file space taken from the client's device.

11.1.2 Possible Programming Languages

There are number of languages to choose from, whether it being Java, C++, Python etc to build a standalone application, I would choose either C++ as I studied it in third year or to use Python. Python is the most popular language nowadays and is seen as the easiest of the programming language.

11.1.2.1 C++

C++ has been around since the 1979 which has acquired a huge community as pointed out by (Schildt, 2003) "It is the preeminent language for the development of high-performance software", there is a lot of online resources available. It is portable, so it can be implemented across a variety of Operating systems. However, it does have its disadvantages. One of the biggest problems with C++ is that there is no automated memory disposal which is an inconvenience. Also, there are security problems with using this old system.

11.1.2.2 Pros and Cons of using C++.

11.1.2.2.1 Advantages	11.1.2.2.2 Disadvantages
Large community	No memory disposal
Portability	Security problems
	Old Technology

11.1.2.3 Python

(Pramanick, 2022) Python, initially created to make writing code easier by Guido van Rossum in 1991, it was designed to for readability and increase in productivity. It was made so that everyone could use it with ease in comparison to other programming languages. Out of all the languages it is also the easiest to learn and takes the least amount of time to become proficient in.

11.1.2.4 Python

11.1.2.4.1 Advantages	11.1.2.4.2 Disadvantages
Large community	Relatively new
Portability	Slower thank compiled languages
Ease of use	Python is dynamically typed
Scalable	

(Bhagat, 2022) I have learned that there are several disadvantages to using Python, being new that it poses security vulnerabilities, its slower than other compiled languages. However, it there is a large community behind it and is being optimised continuously, it can be implemented easily across different platforms.

11.1.2.5 Standalone vs Web Application

There are several differences, one of the major ones being that using a web application would provide availability being always online. User data would be stored on the cloud, and it would allow the application function over several different platforms.

11.1.2.6 Standalone vs Web Application

11.1.2.6.1 Stand Alone	11.1.2.6.2 Web App
Standalone vs Web Application	Always connected to internet
Single process	Continuously saved
Restricted to selected device/devices	Cloud based; no installation required
Don't update regularly	Secured online
	Available on any device

12 Evaluation of the Application

When the application is functioning/complete, I will enquire with several companies in the IT sector if they would like to try the application and give me their opinion on the project on multiple aspects such as sections covered, the questions asked, the length of time to complete the assessment, the viability etc. Understanding the needs of companies directly would benefit the project.

13 Application Security

Depending on the type of application, it would be susceptible to a variety of attacks. It would be easier for distribution of the application if it is web based. When using web based, applications can be susceptible to the following: Cross site scripting (XSS), SQL Injection, Session Fixation, Cross Site Request Forgery (CSRF). Security is a vital aspect of the application to ensure the integrity of the data stored/displayed.

14 Conclusion

Commented [CS3]: Do you need to add something about cyber insurance companies?

Since the pandemic there has been an increase of 600% in cybercrime carried out since the pandemic began (Purplesec 2022). This increase has caused for a largescale working environment change by implementing remote working at a global scale. With so many people working at home it gave threat actors a better chance of infiltrating businesses as stated by (Barker, 2021) “In 93 percent of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources.” Small to medium businesses were a major contributor to breaches, which effects their reputation. By creating a web application using questions that give a descriptive insight into the IT security posture of a potential client. The questions asked are scored using a Qualitative risk assessment determining the weighting of each answer. The questions come from multiple Frameworks such as NIST, ISO 27000 series etc. With hosting the application remotely, it will provide portability to the user to determine their posture with an easy-to-use interface. Providing this application to insurance providers will give great insight as to how well the assessment performs in a live environment and will save time and cost from the insurer’s perspective.

15 Bibliography

2022 cyber security statistics trends & data (2022) *PurpleSec*. Available at: https://purplesec.us/resources/cyber-security-statistics/#WFH (Accessed: November 23, 2022).

2022 cyber security statistics trends & data (2022) *PurpleSec*. Available at: https://purplesec.us/resources/cyber-security-statistics/#Cybercrime (Accessed: November 25, 2022).

A crisis in third-party remote access security (2021) *Securelink.com*. Available at: https://www.securelink.com/wp-content/uploads/2022/08/SL_ResearchReport-Third-Party-Security.pdf (Accessed: November 25, 2021).

Ackerman Jr., R. (2022) *Weak cybersecurity is taking a toll on small businesses*, *Tripwire*. Available at: https://www.tripwire.com/state-of-security/weak-cybersecurity-taking-toll-on-small-businesses (Accessed: November 23, 2022).

Almack, B. (2022) *On the money - online retail H1 2022*, *Wolfgang Digital*. Available at: https://www.wolfgangdigital.com/blog/on-the-money-online-retail-h1-2022/ (Accessed: November 19, 2022).

Barker, I. (2021) *Cybercriminals can penetrate 93 percent of company networks*, *BetaNews*. Available at: https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/ (Accessed: November 25, 2022).

Bhagat, V. (2022) *Pros and cons of python programming language*, *PixelCrayons*. Available at: https://www.pixelcrayons.com/blog/python-pros-and-cons/ (Accessed: November 18, 2022).

Carson, J. (2023) *What is Cyber Insurance and why do you need it?*, *What is Cyber Insurance and Why Do You Need it?* Delinea Inc. Available at: https://delinea.com/blog/what-is-cyber-insurance (Accessed: April 8, 2023).

Chesler, R.D. and Yousef, C. (2016) *Insurance disputes over cyber claims - memberclicks*. Available at: https://coverage.memberclicks.net/assets/CommitteePagesSelectedPapers/accec_cyber_insurancedisputesovercyberclaims-currentandfutureflashpoints_chesleryousef.pdf (Accessed: April 7, 2023).

Coker, J. (2022) *Businesses found to neglect cybersecurity until it is too late*, *Infosecurity Magazine*. Available at: https://www.infosecurity-magazine.com/news/cybersecurity-seriously-breach/ (Accessed: November 19, 2022).

Comerford, L. (2022) Why small businesses are vulnerable to cyberattacks, Security Magazine RSS. Security Magazine. Available at: https://www.securitymagazine.com/blogs/14-security-blog/post/97694-why-small-businesses-are-vulnerable-to-cyberattacks (Accessed: December 7, 2022).

Cronley, T. (2019) *How can IT managers in hi-tech multinationals ensure due diligence is applied to both hardware and software from third-party suppliers to prevent security vulnerabilities*. thesis. The Thesis Centre.

CSRC presentation: NIST Cyber Risk Scoring (CRS) - program overview (2021) *CSRC*. Available at: https://csrc.nist.gov/presentations/2021/nist-cyber-risk-scoring-crs-program-overview (Accessed: November 8, 2022).

Cyber Liability and data security - USLI (2016) *USLI Cyber Liability and Data Security +*. Available at: https://customers.usli.com/sites/dapps/Dapp_Professional_cyberliability.pdf (Accessed: April 14, 2023).

Demand side of Cyber Insurance in the EU (2023) *ENISA*. Available at: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu (Accessed: April 6, 2023).

Donohue, J. (2022) *Third-Party Risk Management Policy: Benefits, Best Practices & How to Create Your Own*, *Diligent Corporation*. Available at: https://www.diligent.com/insights/grc/third-party-risk-management-policy/ (Accessed: November 16, 2022).

Enisa Threat Landscape 2022 (2022) *ENISA*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Accessed: November 25, 2022).

Fig 1: Omer, G. (2022) *Fourth-party security: Another level of security management*, *Panorays*. Available at: https://panorays.com/blog/fourth-party-security-another-level-of-security-management/ (Accessed: November 8, 2022).

Fig 10: Guide to conducting cybersecurity risk assessment for CII (2021). Available at: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf (Accessed: November 17, 2022).

Fig 2: Demand side of Cyber Insurance in the EU (2023) *ENISA*. Available at: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu (Accessed: April 6, 2023).

Fig 3: Carson, J. (2023) *What is Cyber Insurance and why do you need it?*, *What is Cyber Insurance and Why Do You Need it?* Delinea Inc. Available at: https://delinea.com/blog/what-is-cyber-insurance (Accessed: April 8, 2023).

Fig 4: Research Team, C. (2023) *Check point research reports a 38% increase in 2022 global cyberattacks*, *Check Point Software*. Check Point Software. Available at:

https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (Accessed: April 7, 2023).

Fig 5 & 6: *Cyber Liability and data security - USLI* (2016) *USLI Cyber Liability and Data Security +*. Available at: https://customers.usli.com/sites/dapps/Dapp_Professional_cyberliability.pdf (Accessed: April 14, 2023).

Fig 7: Risk Score Results - Determining TPRM (no date) *Prevalent*. Available at: https://www.prevalent.net/risk-calculator/ (Accessed: April 17, 2023).

Fig 8: *Guide to conducting cybersecurity risk assessment for CII* (2021). Available at: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf (Accessed: November 17, 2022).

Fig 9: *Guide to conducting cybersecurity risk assessment for CII* (2021). Available at: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf (Accessed: November 18, 2022).

Fig 10: *Guide to conducting cybersecurity risk assessment for CII* (2021). Available at: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf (Accessed: November 18, 2022).

International ISO/IEC standard 27001 (2013). International Organization for Standardization. Available at: https://www.qal-iran.ir/WebsiteImages/iso/21.PDF (Accessed: April 17, 2023).

International ISO/IEC standard 27002 (2013). ISO/IEC 2013. Available at: http://www.itref.ir/uploads/editor/17df68.pdf (Accessed: April 17, 2023).

Jibilian, I. and Canales, K. (2021) *The US is readying sanctions against Russia over the SolarWinds cyber attack. here's a simple explanation of how the massive hack happened and why it's such a big deal*, *Business Insider*. Business Insider. Available at: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T (Accessed: October 31, 2022).

Lyons, K. (2020) *Google saw more than 18 million daily malware and phishing emails related to covid-19 last week*, *The Verge*. The Verge. Available at: https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams (Accessed: April 7, 2023).

NIST Technical Series Publications (2020) Nist.gov. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Accessed: October 25, 2023).

Omer, G. (2022) *Fourth-party security: Another level of security management*, *Panorays*. Available at: https://panorays.com/blog/fourth-party-security-another-level-of-security-management/ (Accessed: November 8, 2022).

Osborne, C. (2021) *Updated kaseya ransomware attack FAQ: What we know now*, *ZDNET*. Available at: https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/ (Accessed: October 31, 2022).

Park, K. and Sen, S. (2016) *Third-party governance and Risk Management - deloitte*, *Third-party governance and risk management The threats are real*. Available at: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-third-party-governance-and-risk-management-290817.pdf (Accessed: November 15, 2022).

Pramanick, S. (2022) *History of python*, *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/history-of-python/ (Accessed: November 17, 2022).

Ragan, S. (2015) *BitPay insurance claim rejected due to contract wording*, *CSO Online*. CSO. Available at: https://www.csoonline.com/article/2984777/bitpay-insurance-claim-rejected-due-to-contract-wording.html (Accessed: April 7, 2023).

Rahmonbek, K. (2023) *35 alarming small business cybersecurity statistics for 2023*, *StrongDM*. StrongDM. Available at: https://www.strongdm.com/blog/small-business-cyber-security-statistics (Accessed: April 7, 2023).

Ross, R., McEvilley, M. and Oren, J.C. (2016) *NIST SP 800-160*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf (Accessed: November 25, 2022).

Schildt, H. (2003) *C++ A Beginner's Guide*. 2nd edn. New York, United States: McGraw-Hill Education.

Services, E.R.M.F. (2022) *Why you need cyber insurance in ireland • ERM financial services*, *ERM Financial Services • Commercial Insurance Broker Ireland*. Available at: https://ermfinancialservices.ie/cyber-insurance/why-you-need-cyber-insurance-in-ireland/ (Accessed: April 10, 2023).

The top 5 security risks of remote working (2022) *Redcentric*. Available at: https://www.redcentricplc.com/network-security/top-5-security-concerns-of-remote-working/ (Accessed: October 31, 2022).

Warburton, D. (2020) *2020 phishing and fraud report*, *F5 Labs*. Available at: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report (Accessed: October 31, 2022).