FIZZITS security risk assessment

By Joseph Batchelor

Project Scope statement

Project Description

I need to develop and implement a security risk assessment to help refine and make aware of the importance of information security within Fizzit's 10 step quality check process. Additionally, to impede identified threats and maintain the confidentiality, integrity, and availability of information and other essential assets.

Project Objectives

- Create a security risk assessment based on the ISO 27001.
- Produce and implement security polices and controls based on the ISO 27001.
- Evaluate assets and their threats and vulnerabilities using tools and resources.
- Reduce the possibility of threats events and provide mitigation methods.

In Scope

- Fizzit's 10 step quality check process
- Asset table.

Out of Scope

This project's main focus is Fizzit's 10 step quality check process only. Anything outside of this scope will not be part of the current project. Additionally, the following are also considered out of scope:

- Building structure
- Facility utilities

Project deliverables

- Policies, standards, and procedures
- Risk assessment
- Employee contract
- Business continuity plan
- Incident response plan
- Disaster recovery plan
- CVE statement
- Training & awareness

Project Acceptance Criteria

I agree that this is delivered when:

- Successful implementation , distribution and use of policies and controls are used to maintain the operation of a business and reduce the occurrence of risk events.
- Threat occurrence has been reduced by with residual risk occurrence below 10%.
- The confidentiality, integrity and availability of assets are retained.
- The operation of business has not been distributed or negatively affected with the new security implementation.

Projects Constraints

Deadline: 17 December 2021

Context of the organisation

What are Fizzit's goals?

Fizzit's goal is to buy second-hand books, CDs, DVDs, and games from the public via a website and then on-sell them to its parent company The World of Online (TWOO).

Who are Fizzit's customers?

Customers are individuals are who are interested in making money from old books , DVDs, and games they have no use for.

What does Fizzit's offer to customers?

They offer consumers money in exchange for second-hand items. These items are then sold to their parent company which then sells them to the public for an increase fee than the original price. Revenue is generated through a markup of products bought.

Interested parties

Interested party	Internal	External
Owners	**x**	
Employees	**x**	
Senior management	**x**	
Customers		**x**
Competitors		**x**
Suppliers		**x**
Partners		**x**
Government		**x**

SWOT analysis

Strength	**Weakness**
• Strong and effective business model. • Trust pilot score of 5 making them top in that category. • Partner company (WOB) certified by B corp. • Provides a trusted and an efficient service.	• Lack of information security awareness. • Not ISO certified. • No physical interaction or service for computer illiterate individuals (Online only). • Lack of reputation hasn't been established yet.
Opportunity	**Threats**
• Get ISO 27001 certified. • Effective policy development. • Introduce other products to sell such as technology like computers and tv's etc.	• No or lack of an effective risk assessment. • No or lack of effective security policies. • Competition such as eBay pose a threat as they are cutting out the middleman. • Products becoming obsolete (i.e., DVDs & CD's) so demand is low. • Covid 19 has affected the sales of products and operation of business.

Organisational roles

Role	Description
CEO	Chief executive officer is the highest-ranking official within the business.
IT Manager	Responsible for coordinating and leading employees as well as introducing and coordinating IT related activities.
Support Technician	Responsible for installing and configuring systems and identifying faults and or problems with IT assets.
Systems administrator	Responsible for monitoring and fixing server and system problems, they are all responsible for introducing and installing new updates and configurations for systems.
Network administrator	Responsible for everyday network operations while also supporting and maintaining systems on both local and or wide networks. They are also responsible maintenance of network mitigation methods.
Chief technician officer	Works along with the CEO to strategize and anticipate decisions that affect both the business and IT infrastructure.
Chief security Officer	Works with the CEO to implement and introduce safety and security for both assets and employees. Focusing on providing mitigation methods and developing a secure system.
Quality assurance	A specialist that works within the checking process instructed to observe products received and check their overall condition.

Identifying Assets

The understanding and identification of assets used within a business is an important process. This can be used to recognize which assets contribute to key operations of the business and provides clarity of their importance if an undesired event were to occur.

Asset identity table (**Table 1.1**) is used to display all the provided assets that Fizzit's use. This lays out specific details regarding each asset such as their functions and who has authorisation to use it.

Table 1.1 - Asset identity table

Asset type	Name	Function	Version	Vendor	Authorised users	step in process
Database	Microsoft SQL server 2016	House all the data of consumers and employees of the business.	13.0.1601.5	Microsoft	CTO, CSO & Systems administrator	**ALL**
router	Extreme Networks X670V-48T	Provides network connection for all devices as well as a gateway to the internet.		Extreme Networks	CTO, CSO & Network administrator	**ALL**
Web server	AWS	Run and display Fizzit website for consumers to access.		Amazon	CSO, Systems administrator & IT Manager	**9**
Hosting server	HPE PROLIANT ML350 GEN10 SERVER	To virtually run Fizzit's IT services, websites, related data, and applications off premise .	8.4	Hewlett Packard Enterprise	CTO, CSO & Systems administrator	**ALL**
Webform	Amazon EC2	Collects data from users or to provide the ability for user to enter data.		Amazon	Systems administrator & IT Manager	**ALL**
Server operating system	Windows Server 2016	Hosting server that allows the ability to operate and use the servers.	10514.0.150808-1529	Microsoft	CTO, CSO, Systems administrator, Support Technician & IT Manager	**7,8**
Desktop computer	HP EliteDesk 705 G3	Used for inputting data and communication.		HP	CTO, CSO, Quality assurance, Support Technician & IT Manager	**7,8**
Scanner	WASP barcode scanner	Scans barcodes and is able to send that data to other devices.		RS Component Ltd	CTO, CSO, Quality assurance, Support Technician & IT Manager	**2**
Barcode reader app	Inventory System	Scan barcodes or QR codes of books used to send and collect information.		asap systems Ltd	CTO, CSO, Quality assurance, Support Technician & IT Manager	**2**
Data	Employee emails	Personal information that allows for the transfer and communication between employees and managers.		Fizzit	Quality assurance, IT Manager & Employees	**ALL**
Data	Employee personal data	Employee personal data is stored to maintain information about how to contact , who they are and any specific requirements.		Fizzit	Quality assurance, IT Manager & Employees	**ALL**
Data	Customer personal data	Customer data is stored to be used to easily identify, contact, and obtain payment from them.		Fizzit	Quality assurance, IT Manager & Employees	**ALL**
Data	Customer Email's	Used to contact customers as well as to keep them up to date with news from the business.		Fizzit	Quality assurance, IT Manager & Employees	**ALL**
Data	Product information	This information that is stored describing each assets details. Such where it came from and where it's going.		Fizzit	Quality assurance & Employees	**2**
Physical	Products	These are the products that Fizzit are selling through the world On Online to make capital.		Fizzit	Quality assurance & Employees	**ALL**
Human	Employee's	These ae low hierarchy business workers that perform		Fizzit	N/A	**ALL**
Human	Managers	These are the mid-level employee who are tasked to maintain operation and communication with low level employees.		Fizzit	N/A	**ALL**
Human	Administrators	An individual who is responsible for carrying out duties for the business IT systems.		Fizzit	N/A	**ALL**
Human	CEO	The highest-ranking individual who manages the overall operation.		Fizzit	N/A	**ALL**
Human	Customer	The clients that help generate revenue and money for the business.		Fizzit	N/A	**N/A**
Data	batch file script	Used to updated once a week all the products purchased by Fizzit.		Fizzit	N/A	**N/A**

Asset valuation

Determining the value of assets helps businesses calculate the priority of assets. Doing so can help both the development and deployment of security controls for specific assets. Being able to accurately valuate assets allows businesses to plan for undesirable events and allows them to adjust accordingly and effectively to minimize impact to both the operation and costs of the business.

Classification based valuation table (**Table 2.1**) this table will be used to provide qualitative data for determining the overall value of an asset. The table will describe the impact of different critical levels an asset would have if it were to be unavailable.

Table 2.1 - Classification based valuation table

Criticality level	Impact
Critical	A critical level asset is one that if compromised the asset would have serious consequences which may lead to the loss of life and or serious injury. Additionally, this can disrupt the overall operation of the business and critical functions.
High	A high-level asset is one that if compromised would have serious consequence that may impair critical functions and can affect the operation of the business for long term.
Medium	A medium level asset would be one where if failure were to occur this asset would cause moderate consequences operation of the business for a short/mid duration.
Low	A low classification can have little or no impact of the operation of the business but may affect the efficiently and effective of completing tasks.

Asset valuation table (**Table 2.2**) uses qualitative data for determining the priority of assets based on the critical level. This provides detail to the importance of assets they have to the operation of the business.

Table 2.2 - Asset valuation table

Asset name	Product name	Criticality level
Database	Microsoft SQL server 2016	High
router	Extreme Networks X670V-48T	High
Web server	AWS	High
Hosting server	HPE PROLIANT ML350 GEN10 SERVER	High
Webform	Amazon EC2	Medium
Server operating system	Windows Server 2016	Medium
Desktop computer	HP EliteDesk 705 G3	Low
Scanner	WASP barcode scanner	Low
Barcode reader app	Inventory System	Low
Data	Employee emails	Low
Data	Employee personal data	High
Data	Customer personal data	High
Data	Customer Email's	Low
Data	Product information	Low
Product	Products (CD, DVD'S & Books)	Medium
Human	Employee's	Medium
Human	Managers	Medium
Human	Administrators	Medium
Human	CEO	High
Human	Customer	High
Data	batch file script	High

Identifying threats

This section discusses and identities the necessary threat agents and threat events to both Fizzit assets and their quality checking process. This is used to help inform and educate employees and the company of the possible sources of attacks as well the type of threat that exist and what they do.

Threat agents table (**Table 3.1**) is designed to provide clarity of the potential threat agents that Fizzit may face. I separated the sources into categories so that understanding the spread of attack can come from different sources. This allows me to develop controls that Specifically target these threats categories as some may not be as relevant as others.

Table 3.1 - Threat agents table (by type and category)

Threat agents		
Human	**Environment**	**Technology**
• Intruder • Outsider • Hacker • Terrorist • Competitor • Customer • Vendor • Employees • Insider • Ex-employee	• Fire • Rain • Flood • Hurricane • Tsunami • Snow/ice • Earthquake • Tornado • Lightning • Weather	• Infrastructure • Power • Network • interference • Internet • Application • Software • Hardware • Operating system • Telecommunication

Threat severity classification table (**Table 3.2**) is designed to provide an understating of the impact that some threats may have to the business. This also provides a quantitative score that will be used to determine threats that should be implemented with the risk assessment.

Table 3.2 - Threat Severity classification table

Severity	Impact
9 - 10	This is a threat that can compromise assets and disrupt critical business operations over long term as well cause loss of life or serious injury to people.
6 - 8	These are threats that compromise assets with the result of impairing systems and devices as well as disrupting the operation of a business for short term.
3 - 5	This is a threat that if it was to compromise an asset it will have moderate consequences that would impact the efficiency and effectiveness when completing tasks and the overall operation of the business.
0 - 2	This is a threat that would have little or no effects on the operation of the business and may disrupt low level functions from being completed.

Severity level acceptance

An acceptable level of risk severity for Fizzit would be anything below the value 5. Due to the fact that they are short term consequences which do not pose a serious threat to Fizzit other than causing small financial implications, does not pose a significant threat. Values beyond 5 can either impair critical assets, disrupt the operation of the business, and could potentially inflict serious harm to people and even cause loss of life this can cause long term problems which can affect the overall operation of the business as well as inflict large financial problems. Additionally, Fizzit should consider the importance of critical assets such as employees and the affect it would have on them.

Threat identify table Business generalised (**Table 3.3**) identifies a generalised set of threats that can occur across the entire business. I created this category as this highlight's common threats across different assets such as hardware ,software or the facility itself.

Table 3.3 - Threat Identity table (Business generalised)

Threats	Threat Description	Severity	C	I	A	Implementation Justification
Ineffective security measures	Implemented measures, tactics and procedures designed for protection however fail to protect the confidentiality, integrity, and availability of IT components.	9	X	X	X	• A weakness of Fizzit is the lack of security awareness therefore security measures may not be suitable can be a potential threat.
Back up failure	Failure to backup due to undesirable event which prevents the possible process of maintaining data and information or different device / location.	4			X	• Affects information security. • Can disrupt the operation of the business by making some data unavailable.
Environmental damage	This is the possible occurrence of an undesirable environmental event such as Fire, Rain, Flood and or Hurricane that can physically damage or disable critical systems.	7		X	X	• This can impact the business in multiple ways such as financial and operational.

						• The potential loss of data and hardware and system damage can limit key functions.
Improper training and protocols	This is where there is a lack of or inefficient training / education for employees. This can result in an overall weak security and or improper understanding on mitigation methods and attacks.	5	X			• This can have a long-term impact on employees which why it's been identified. • If employees do not receive the proper training, then there is a chance for more errors to be made.
Data breach	This is when data stored within a media such as a desktop or database is compromised and stolen, viewed, and copied by an unauthorised user or threat agent	7	X		X	• Common attack within businesses • Can be accomplished through most of the assets Fizzit have. • Can be detrimental for information security. • Affects the Confidentiality of data stored.
Exposure of backup data	This is a potential threat where a data backup source is unavailable and or intercepted and that the data stored has been stolen and or un-accessible.	3		X	X	• Can affect data and information being stored which affects information security. • Can disrupt the operation of the business.
Unauthorized Intruder	This is when an external threat agent gains unauthorised access to a system or the premise with the use of false credentials or the use of stolen legitimate credentials.	7	X	X	X	• Because Fizzit sells different products and has a facility of different hardware and systems the possibility of a thief is high.
Weak or lack of security policy	This is when a business fails to provide necessary or efficient policies or that they may not provide enough policies to cover the overall scope of what needs protecting.	8	X	X	X	• Due to a previous weakness of Fizzit which is the lack of security awareness therefore security policies may not be as effective.
Not ISO certified	Being certified provides that management systems, manufacturing process and other procedures all have standardization and quality assurance to ensure overall consistency. by not being or losing your certification can reputational damage to your business.	2				• These is no evidence that Fizzit have been ISO certified which can be a threat to the business if not.
Disabled systems	This is an attack that slows or even disables a database from being access. By temporary taking down the targeted system by flooding it with traffic.	10		X	X	• Some threats that are listed for assets have the potential to impair system which can make them unavailable.
Weak audit	This is the failure of collecting detailed and premise data which can result in insufficient data or information for protecting your organisation.	5		X		• Not being able to get detailed information after an undesired event can be a problem, as this can help you in the future.

Threat identify table Human assets (**Table 3.4**) Identifies the threats associated with human assets that can occur within Fizzit's business.

Table 3.4 - Threat Identity table (Human assets)

Threats	Threat Description	Severity	C	I	A	Implementation Justification
False authentication	The use of illegitimate credentials or fake credentials to gain unauthorised access.	3	X			• A common method for attackers to trick employees in the process of gaining information. • Can be easy to perform if weak or lack of security measures are used.
Unauthorised access	When a threat agent gains access to a restricted system, software, data, or area without permission.	9	X	X	X	• A common threat that can be done by employees intentionally or accidentally. • Employees can be tricked into performing unauthorised tasks.
Inappropriate use of IT equipment	This is when employees and or threat agents intentionally use a piece of equipment not for its intended purposes.	7	X	X	X	• This can lead to serious damage or loss of life if not controlled. • Typically, CMA crimes are caused by inappropriate use of systems.
Social engineering	This is a threat where a threat agent is able to manipulate employees to perform certain actions or provide confidential information.	4	X			• A very common cyberthreat which occurs in most successful attack and or breaches.
Weak Authentication	The use of weak credentials can be a threat to a database and or other systems. This threat can allow threat agents to gain access with the use of password or authentication cracking methods.	4	X			• Most employees will have to use a form of authentication with the use of specific credentials. • Depending on the role of the user they may have a high clearance which can be a problem if they use weak credentials.
Sabotage	This is the intentional damage or action by an internal threat agent which can impair systems and or cause loss of life.	8	X	X	X	• This can be an act that can be serious for employees' lives. • Can also be the cause of an employee.

Theft of equipment and information	This is when an internal or external threat agent takes business's property without authorisation.	6		X	X	• Employees are able to easily steal equipment due to having the ability of onsite access. • Employees who are convicted of CMA crimes typically steal information.
Phishing	This is the process of sending fraudulent communications that appear to come from legitimate sources with the intent to obtain confidential / sensitive information.					• Common attack that targets employees. • A typically starting method introduce detrimental threat like ransomware.
Station hijacking	This is the physical process of using another user's workstation without authorisation or permission.	4	X			• A threat which happens in most CMA crime cases for unauthorised access to information.
Keyloggers	These are physical devices are installed on devices to obtain the keystroke users enter on a system. Typically used to obtain credentials.	4	X			• Can be used to obtain employee credentials. • Are easily installed and hidden.
Spyware	This is malicious software that is designed to monitor and gather data from systems without the user knowledge.	4	X			• Can be used to obtain employee credentials. • Are easily installed and hidden within systems.
Masquerading	This is when a person imitates someone else identity and using legitimate sources to carry out attacks.	3	X			• A very common cyberthreat which occurs in most successful attack and or breaches. • Employees can use this threat on consumers.
Eavesdropping	A threat that occurs when a hacker or individual intercepts data between devices or in person.	4	X			• A threat which happens in most CMA crime cases for unauthorised access to information
Replay attack	A threat where attackers intercept messages or data and doing so is able to delay and or modify it before sending it to the receiver.	4	X			• A possible threat that can occur within Fizzit operation.
Impersonation attack	This is an attack where the attack impersonates a legitimate user or employee to gain access to unauthorised material.	4	X			• A very common cyberthreat which occurs in most successful attack and or breaches. • Employees can use this threat on consumers.

Threat identity table Hardware & software (**Table 3.5**) identifies all the relevant threats that can appear from Fizzit's assets. This threat selection was added as the assets play an important role within Fizzit business as some of the assets below provide critical operation for important functions to be completed. Additionally, these assets also make an appearance within Fizzit's quality check process.

Table 3.5 – Threat identity table (Hardware & software)

Threats	Threat Description	Severity	C	I	A	Implementation Justification
SQL injection	This is an attack that injects malicious code through a web site (Front end) which is then passed to the database to perform detrimental actions.	7	X			• Common attack within businesses • Can affect information assets • Common across most Fizzit assets • Can be detrimental for information security. • Affects the Confidentiality of data stored.
Excessive privileges Abuse	This is when database users have access that exceeds their privileges. They may abuse this to access and or modify the content of data through unauthorised means.	4	X			• Targets data which affects information security. • Attack surface is large due to various number of users. • Can affect the integrity and confidentiality of data.
Denial of service attack	This is an attack that slows or even disables a database from being access. By temporary taking down the targeted system by flooding it with traffic.	10		X	X	• Detrimental to all assets. • Can impact the operation of the business. • Can affect critical functions. • Is capable of disconnecting and segregating the network and components.
Configuration errors	Deliberate Errors when configuring your database such as settings, or controls not set correctly can be a simple way of attracting threats.	6		X		• An easy threat to accomplish. • Can be done physically or digitally through the network. • Can cause serious problems and open up vulnerabilities. • Can be done to multiple systems.
Privilege escalation	This is when attackers take advantage software vulnerabilities to turn the access privileges from an ordinary user to an administrator.	4	X			• A common vulnerability with Fizzit assets. • Can be used to access high level clearance data and or access critical systems. • A typical starting point for most attacks.
Unauthorized access	This is when a person gains entry to a computer , system, or network without permission	7	X			• Common attack across assets. • A typical process threat agents perform. • Can affect the confidentiality and integrity of information. • Affects information security.
Rerouting	This is an attack that redirects traffic from legitimate point to a false point.	7	X		X	• A common web attack. • Can affect both employees and consumers. • Can be easily done.

Information theft	This is when an individual or devices extracts data from a database or to steal physical copies.	7	X			• Common attack across assets. • Affects information security. • Fizzit can develop a bad reputation from it. • Can be done by internal and external agents. • Does not require technical attacks.
Password attack	This is a collection of password base attacks such as brute or dictionary attack used to enter systems without authorisations.	4	X			• Most assets implement password protection. • Employees also implement password protection. • Can affect information security.
Packet sniffing	This attack is the theft and or interception of data within a network. Designed to capture network traffic using a packet sniffer.	6	X	X		• Most assets are connected to the network which means that their transmissions can be intercepted. • Affects information security. • Can target both employees and consumers.
Cross site scripting	This is an attack that injects malicious scripts into a web page to be sent to an unexpected user.	8	X			• A common web attack that most webpages face. • Can target both employees and consumers. • Can be detrimental if performed effectively.
Virus & worms	These are malicious programs that replicates from one device to another without the user being aware.	4	X	X	X	• Can disable critical systems. • Affect he operation and impar critical functions. • Can have multiple attack vectors. • Can spread across to other assets.
Botnets	This is a network of multiple computers that are being controlled from a single point to perform different attacks.	6		X	X	• Detrimental to all assets. • Can impact the operation of the business. • Can affect critical functions. • Can perform multiple attack as once.
Ransomware	This is a type of malware that is designed to hold victims' information at random. Until a payment is made.	7	X	X	X	• Detrimental to all assets. • Can impact the operation of the business. • Can affect critical functions. • Can cost a lot of money to remove. • Can be easy installed due to employees.
Cross site request forgery	This is an attack that tricks an authenticated user to enter unwanted actions on a website.	4	X			• A common web attack that most webpages face. • Can target both employees and consumers. • Can be detrimental if performed effectively.
Spam attacks	This is an attack that bombards am email system or user with bulk messages to prevent access.	4			X	• Detrimental to all assets. • Can impact the operation of the business. • Can affect critical functions. • Can make services and applications unavailable.
Broken authentication attacks	These are different attacks where attackers are able to compromise legitimate credentials to gain unauthorised access.	7	X			• High possibility of occurrence • Can used across multiple assets.
Buffer overflow	This attack targets the memory block of a system or device. This is done when large amounts of data is entered beyond the fixed length enters its adjacent memory space which attackers to overwrite the data held within.	3		X	X	• A common attack that can happen to most systems running an OS • Affects information security. • Can damage hardware of assets.
Injections (XML , etc)	The use of malicious code that is injected through network and devices to obtain information and data form a database.	7	X			• Common attack within businesses • Can affect information assets • Common across most Fizzit assets • Can be detrimental for information security. • Affects the Confidentiality of data stored.
Unsecured Wi-Fi points	These are malicious Wi-Fi points disguised as legitimate points to trick individuals to sign on and share malicious code or obtain information.	4	X			• Can be easily performed with custom devices. • Most assets need connection to a network which means that their transmissions can be intercepted if they were to connect to that access point.
Trojan horse	This is malicious code / software that is designed to brute force into systems to gain access.	6	X	X	X	• Is able to impact the entire CIA triad. • Can have different forms and use different attack vectors to cause damage.

Threat identify table Quality check process (**Table 3.6)** identifies the threats that may occur within the quality check process. This also provides a different view of impact that these threats can have on the business. I felt it was relevant to provide a different perspective of how the business could be affected negatively by threats.

Table 3.6 - Threat Identity table (Quality check process)

Threats	Threat Description	Severity	Financial	reputational	Operational	step in process	Implementation Justification
Theft of products	This threat is the process of Products being stolen by certain threat agents.	5	X	X		1,3,	• Fizzit business model is based on selling products to make money, if they lose products, they lose money.
Damage to products	This threat is the accidental or intentional damage of consumer products during the checking process.	4	X	X		1,2,3,4	• If Fizzit are unable to sell product due to them being damaged, then they are unable to make money from that.
Counterfeit products	These are fake replicas of products in the attempt to be passed as legitimate products.	4	X			2,3	• Fraudulent products are a common problem for e-retailers which can impact them finically.
Delivery / operation disruption	When delivery or operation is disrupted by an undesirable, political and environmental event.	8	X		X	1	• A recently common threat due to Covid-19 which can cause this threat.
Manipulation of data	This threat is the process of intentional or accidental alteration of data when entered within the system.	6			X	5,6	• Employees can potentially perform this threat and is a common reason with CMA.
Weak examination	This threat is the process of ineffectively or incorrectly examining the integrity of product received.	7			X	3	• Human error is a common possibility with most employees.
False / mistaken insertion of data	This threat is the accidental or intentional insertion of inaccurate or correct data within a system.	5			X	5,6	• Human error is a common possibility with most employees.
False acknowledgement	This threat is the intentional or accidental acknowledgement of entering damaged product the system.	6		X		4,5,6	• Human error is a common possibility with most employees.
Disable systems	This is the occurrence of an attack that disables the use of critical systems such as the database preventing access to these systems.	9			X	2,7,8	• This can happen if one of the assets were to fail due to an attack.
Fraud	This is when consumers attempt to perform fraudulent actions with the attempt to deceive other with the intent to be compensated.	8	X		X	2,3,7	• Fraudulent products are a common problem for e-retailers which can impact them finically.

Threat mapping to assets table (**Table 3.7**), is designed to show which threats can affect which assets. Most threats can appear within multiple assets which can be a problem but also a useful indication of the Severity of impact that threat may have on Fizzit.

Table 3.7 - Threat mapping to assets table

		Assets																			
		Microsoft SQL server 2016	Extreme Networks X670V-48T	AWS	HPE PROLIANT ML350 GEN10 SERVER	Amazon EC2	Windows Server 2016	HP EliteDesk 705 G3	WASP barcode scanner	Inventory System	Employee emails	Employee personal data	Customer personal data	Customer Emails	Product information	Products (CD, DVDS & Books)	Employees	Managers	Administrators	CEO	Customers	Batch file script
	SQL injection	X		X	X	X				X	X	X	X	X	X		X	X	X	X	X	X
	Excessive privileges abuse	X	X					X				X	X		X		X	X	X	X	X	X
	Denial of service attack	X	X	X	X	X	X	X		X	X						X	X	X	X	X	X
	Configuration errors	X	X	X	X			X	X	X	X	X	X	X	X						X	X
	Privilege escalation	X	X		X	X	X	X	X	X		X	X									X

	Unauthorized access	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Rerouting		X	X	X	X					X			X			X	X	X	X	X	
	Information theft	X	X			X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	
	Replay attack		X	X	X	X											X	X	X	X	X	
	Password attack	X		X	X			X														
	Packet sniffing attack		X	X	X							X	X		X		X	X	X	X	X	X
	Cross site scripting			X	X	X											X	X	X	X	X	
	Virus & worms	X	X	X	X			X									X	X	X	X	X	
	Botnets	X	X	X	X			X														
	Ransomware	X		X	X			X			X	X	X	X	X	X	X	X	X	X	X	
	Cross site request forgery					X											X	X	X	X	X	
	Spam	X	X	X	X	X	X	X									X	X	X	X	X	
	Buffer overflow	X		X	X		X	X														
	Injections (XML , etc)	X						X		X												
	Unsecured Wi-Fi points		X						X	X							X	X	X	X		
	Trojan horse		X	X	X			X		X												
	Theft of products														X	X	X	X	X	X	X	
	Damage to products														X	X	X	X	X	X	X	
	Counterfeit products															X	X	X	X	X	X	
	Delivery / operation disruption																X	X	X	X	X	
	Manipulation of data											X	X	X	X	X	X	X	X	X	X	X
	Weak examination															X	X	X	X	X	X	
	False / mistaken insertion of data											X	X	X	X	X	X	X	X	X	X	X
	False acknowledgement																X	X	X	X		
	Disable systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Fraud															X	X	X	X	X	X	
	False authentication																X	X	X	X		X
	Inappropriate use of IT equipment	X	X	X	X	X	X	X	X	X	X											
	Social engineering																X	X	X	X	X	X
	Weak Authentication	X	X	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X	X
	Sabotage	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
	Theft of equipment and information		X		X		X	X	X		X	X	X	X	X	X	X	X	X	X	X	
	Phishing										X	X	X	X	X		X	X	X	X	X	
	Station hijacking																X	X	X	X		X
	Keyloggers							X	X		X	X	X	X	X		X	X	X	X		X
	Spyware							X	X		X	X	X	X	X		X	X	X	X		X
	Masquerading										X	X					X	X	X	X	X	X
	Eavesdropping										X	X			X		X	X	X	X	X	
	Replay attack		X	X	X			X			X	X	X	X			X	X	X	X	X	
	Impersonation attack											X	X				X	X	X	X	X	
	Ineffective security measures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
	Back up failure	X										X	X									x
	Environmental damage	X	X	X	X	X	X	X	X	X						X						X
	Improper training and protocols																X	X	X	X	X	X
	Data breach	X									X	X	X	X	X		X	X	X	X	X	X
	Exposure of backup data																					X
	Unauthorized Intruder	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X						X
	Weak or lack of security policy																			X		
	Not ISO certified																			X		
	Weak audit																			X		

Identifying vulnerabilities

Common vulnerability classification table (**Table 4.1**) uses the common vulnerability scoring system which is an industry standard approach to assessing the severity of vulnerabilities a system may have.

Table 4.1 -Common vulnerability classification table

CVSS	Impact
Critical (8.0 – 10.0)	This is a vulnerability can cause critical damage to the asset and affect all elements of the CIA triad (confidentiality, integrity, and availability).
Medium (4.0 – 7.9)	A vulnerability that can cause damage to the asset and affect some elements of the CIA triad (confidentiality , integrity, and availability).
Low (0.1 – 3.0)	This is a vulnerability that may inflict damage to the asset and affects one of the elements of the CIA triad (confidentiality , integrity, and availability).

Common vulnerabilities and exposure table Hardware & Software (**Table 4.2**) identifies all the relevant and recent hardware and software vulnerabilities that Fizzit assets could be exploited by. These technical vulnerabilities were found using CVE Mitre (*Search CVE list, 1999*) which easily identifies vulnerabilities. For determining the CVSS score I used First.org (*Common Vulnerability Scoring System Version 3.1 Calculator, 2015*) which provides a calculator used to determine the severity score of vulnerabilities.

Table 4.2 - Common vulnerabilities and exposure table (Hardware & Software)

Name	Product	CVE name	CVE Description	CVSS
Database	Microsoft SQL server 2016	CVE-2017-8516	Improperly enforces MS permissions analysis services to disclose confidential information.	5.1
		CVE-2016-7251	A remote XSS attack which injects arbitrary scripts via an unspecified parameter.	5.9
		CVE-2016-7249	An improper cast of an unspecified pointer which allows remote authenticated users to gain privileges.	5.7
Router	Extreme Networks X670V-48T	CVE-2018-5797	A hardcoded AES key that can be used for packet decryption which can be used for access cleartext credentials via a wired port.	7.5
		CVE-2018-5796	A hidden root shell access by entering the administrator password conjoined with the 'service start-shell' CLI command.	8.2
Hosting server	HPE PROLIANT ML350 GEN10 SERVER	CVE-2021-29213	A local attack that bypasses security restrictions to disclose sensitive information and perform a denial-of-service attack and compromise overall system integrity.	7.8
		CVE-2020-7207	A physical attack that targeted the motherboard which can allow privilege escalation with the use of Innovation Engine.	4.1
		CVE-2018-7117	A remote XSS attack which targets the web user interface to obtain confidential information.	7.4
webserver server	AWS	CVE-2021-40527	An attack access developer files via remote access of files stored on the mobile application which allows for the access of confidential credentials.	5.3
Webform	Amazon EC2	CVE-2020-2188	Missing permission check that allowed attackers to access credentials stored in Jenkins	6.5
		CVE-2020-2186	A cross-site request forgery vulnerability that allowed attackers to make Jenkins instances available to them.	6.9
		CVE-2020-2185	No validation of SSH host keys when connecting agents, allowing for a man in the middle attack.	6.5
Server operating system	Windows Server 2016	CVE-2019-0570	Privilege escalation occurs when windows runtime in improperly handles objects within the memory	6.2
		CVE-2019-0584	A remote execution when windows DB improperly handles objects within the memory.	7.5
Desktop computer	HP EliteDesk 705 G3	CVE-2016-2243	Local users are able to cause a BIOS recovery failure (denial of service) by leveraging administrative access.	6.1
		CVE-2012-0697	A default account that allows remote attackers to perform administrative tasks.	6.5
		CVE-2011-4788	Attackers uses external input to construct a pathname entered in the URL which allowed access to confidential files.	7.4
Scanner	WASP barcode scanner	CVE-2019-13526	Remote execution of arbitrary code due to authentication bypass.	6.5
		CVE-2019-12503	Due to unencrypted and unauthenticated data communication, made it prone to keystroke injection attacks.	8.0
		CVE-2014-6869	Prone to man in the middle attack's due to ineffective verification of certificates from SSL servers. Allowed attackers access to sensitive information.	6.5
Barcode reader app	Inventory system	CVE-2021-41256	A security issue by which a malicious application installed on the same device can send it an arbitrary Intent that gets reflected back, unintentionally giving read and write access to non-exported Content Providers.	4.1

Common vulnerabilities Human, Data & product(**Table 4.3**) identifies all the relevant Human, Data & product vulnerabilities that could be exploited during the operation of Fizzit. These were selected because these were common weaknesses that typically occur within business according to OWASP (Vulnerabilities | OWASP, 2021).

Table 4.3 - Common vulnerabilities (Human, Data & product)

Asset type	Vulnerability	CVSS
Data	Data not being encrypted from plaintext.	5.0
	Data not securely stored and being left available.	5.9

	Transmitting data through an unsecured or untrusted mediums.	8.0
	Unreliable devices or hardware used to store or backup data.	5.9
Human	Fall victim to a social engineering attack.	5.3
	Being tricked into opening a phishing email.	5.9
	Making Human errors while at work and not fixing or amending them.	4.1
	Not locking doors or logging out of systems.	5.9
	Using weak credentials on multiple systems.	5.6
Product	Products left out in the open without anyone knowing.	5.7
	A product not properly examined.	4.3
	Not being secured when being delivered	4.3

Risk assessment

Risk level table (**table 5.1**) is used to identify how serious some risks may be to the business. By using financial data this can provide a clear insight of how much the business would need to invest to mitigate that risk. The section in blue highlights the scope of risks that are not tolerated if they were to occur. Anything outside of the scope can be tolerated and paid for due to their low value. The reason the highlighted risks are not tolerated is due to the fact that they are expensive and that if they were to occur regularly this would negatively affect Fizzit finances and so a better approach would be to implement controls to prevent them from occurring.

Table 5.1 – Risk level table

		Probability				
		Very low	**Low**	**Medium**	**High**	**Very High**
Impact	**Very Low**	£100	£200	£1000	£5000	£10000
	Low	£500	£1000	£5000	£25000	£50000
	Medium	£1000	£2000	£10000	£50000	£100000
	High	£5000	£10000	£50000	£250000	£500000
	Very High	£10000	£20000	£100000	£500000	£1000000

Risk evaluation table (**table 5.2**) this table obtains all the information from the previous tables (3.3, 3.4, 3.5, 3.6, 4.2 and 4.3) to construct a risk assessment which identifies all the vulnerabilities and threats that have been given a high score as well as any common risks. The probability of risks have been determined based on complexity of attack, resources needed, and exploitation needed. For example, a risk which requires no resources , low complexity and no exploitation would most likely occur. Impact is determined based on what areas of the CIA triad does it impact, how easy is it to mitigate and the total financial impact.

This table also introduces controls from both annex-a and some specific controls to mitigate risks. The priority of risks have been determined with the use of the Risk level table (**table 5.1**), assets that are not within our tolerance and have a high risk level will be given a high priority compared to those that are tolerated and have a low risk level.

Table 5.2 - Risk evaluation table

ID	Risk Description	C	I	A	Risk Owner	Proposed Controls	Prob	Impact	Risk level	Allow	Priority
1	(**Software**) An external hacker has performed a denial-of-service attack and has disabled the use of Fizzit's Microsoft SQL server 2016 database making data and applications unavailable.		**X**	**X**	IT Manger System admin Network admin	- Black listing IP addresses - Management of technical vulnerabilities(A.12.6.1) - Network controls(A.13.1.1) -Segregation in networks(A.13.1.3)	Med	Very High	£100,000	N	Very High
2	(**Human**) An employee using weak credentials on their HP EliteDesk 705 G3 making it easy for attackers to brute force access.	**X**			IT Manger System admin Chief technician officer	- Implement multi-factor authentication - Automated scanning for weak passwords - Information security awareness, education, and training(A.7.2.2) - Use of secret authentication information(A.9.3.1) - Secure log-on procedures(A.9.4.2) - Password management system(A.9.4.3) - Information access restriction(A.9.4.1)	High	Med	£50,000	N	High
3	(**Software**) A hacker as performed an SQL injection on Fizzit's Amazon EC2 webform where confidential data has been retrieved from the database.	**X**	**X**	**X**	Support Technician Network admin	- Threat detection installation - Use prepared statements - Use stored procedures - Perform input Validation - Enforcing least privilege - Management of technical vulnerabilities(A.12.6.1)	Med	High	£50,000	Y	High

						- Network controls(A.13.1.1) - Security of network services(A.13.1.2) - Segregation in networks(A.13.1.3) - Responsibilities and procedures(A.16.1.1) - Reporting information security events(A.16.1.2) - Reporting information security weaknesses(A.16.1.3) - Response to information security incidents(A.16.1.5)					
4	(**Human**) An external intruder has entered the premise using false credentials and has stolen products and or assets.	**X**			IT Manger CEO	- Introduce CCTV cameras around the premise. - Regularly update locks -Introduce remote monitoring - Access control policy(A.9.1.1) - User registration and de-registration(A.9.2.1) - Physical security perimeter(A.11.1.1) - Physical entry controls(A.11.1.2) - Securing offices, rooms, and facilities(A.11.1.3) - Equipment siting and protection(A.11.2.1) - Unattended user -equipment(A.11.2.8)	Med	Med	£10,000	Y	Med
5	(**Human**) The quality assurance person is a victim of a man in the middle attack between themselves and customer relationship department.	**X**			IT Manger	- Communication verification - Implement a VPN - Information transfer policies and procedures(A.13.2.1) - Agreements on information transfer(A.13.2.2) - Electronic messaging(A.13.2.3) - Securing application services on public networks(A.14.1.1) - Privacy and protection of personally identifiable information(A.18.1.4)	Med	Med	£10,000	Y	Med
6	(**Software**) A hacker performing a cross site script attack on Fizzit's Amazon EC2 webform and has infected a customer and or an employee's session.	**X**		**X**	IT Manger Support Technician System admin	- Filter input on Arrival -Encode data on Output -Implement appropriate headers - Content security policy - Information security awareness, education, and training(A.7.2.2) - Management of technical vulnerabilities(A.12.6.1) - Restrictions on changes to software packages(A.14.2.4) - Reporting information security weaknesses(A.16.1.2) - Privacy and protection of personally identifiable information(A.18.1.4)	Low	High	£10,000	Y	Low
7	(**Human**) An employee has installed ransomware from an email and has infected Fizzit's HP EliteDesk 705 G3 and is now inaccessible.		**X**	**X**	IT Manger Support Technician System admin Network admin Chief technician officer	- Implement an instruction detection system - Configure endpoints - Controls against malware(A.12.2.1) - Installation of software on operational systems(A.12.5.1) - Management of technical vulnerabilities(A.12.6.1) - Restrictions on software installation(A.12.6.2) - Segregation in networks(A.13.1.2) - Assessment of and decision on information security event(A.16.1.4) - implementing information security continuity(A.17.1.2)	Med	Very High	£100,000	N	Very High
8	(**Human**) An employee accessing the Microsoft SQL server 2016 database and looking at confidential data without authorization.	**X**			IT Manger System admin Chief technician officer	-IP whitelisting - Single sign-on - Implement multi-factor authentication - Information security roles and responsibilities(A.6.1.1) - Segregation of duties(A.6.1.2) - Terms and conditions of employment(A.7.1.2) - Information security awareness, education, and training(A.7.2.2) - Disciplinary process(A.7.2.3)	Very High	Med	£100,000	N	Very High

						- Termination or change of employment responsibilities(A.7.3.1) - Access control policy(A.9.1.1) - User registration and de-registration(A.9.2.1) - User access provisioning(A.9.2.2) - Removal or adjustment of access rights(A.9.2.6) - Information access restriction(A.9.4.1) - Confidentiality or nondisclosure agreement(A.13.2.4) - Privacy and protection of personally identifiable information(A.18.1.4)					
9	(**Human**) The quality assurance person has been a victim of social engineering attack where the attacker has impersonated an individual from the relationship department.	**X**			IT Manger	- Spam Filter - Social engineering prevention &training - Threat training and education - Communication verification	Med	Low	£1,000	Y	Very Low
10	(**Human & hardware**) An insider performs a keystroke injection on the Wasp barcode scanner due to a vulnerability were unencrypted and unauthenticated data communication, causing it to be unavailable.			**X**	IT Manger Support Technician	-Perform input Validation - Equipment maintenance(A.11.2.4) - Unattended user equipment(A.11.2.8) - Controls against malware(A.12.2.1) - Management of technical vulnerabilities (A.12.6.1)	Low	Med	£5,000	Y	Very Low
11	(**Hardware**) An insider exploits HP EliteDesk 705 G3 vulnerability where they retrieve confidential files by constructing a pathname entered in the URL .	**X**			IT Manger Support Technician System admin Chief technician officer	- Update OS and software - Secure log-on procedures(A.9.4.2) - Physical security perimeter(A.11.1.1) - Protecting against external and environmental threats(A.11.1.4) - Equipment siting and protection(A.11.2.1) - Unattended user equipment(A.11.2.8) - Management of technical vulnerabilities(A.12.6.1) - Segregation in networks(A.13.1.3) - Protection of records(A.18.1.3)	Low	Med	£2,000	Y	Very Low
12	(**Data**) An insider misconfigured the batch file script that is used to update products on TWOO's database regularly. This can be compromised to perform detrimental damage or SQL injections for customer personal data.	**X**	**X**	**X**	Support Technician System admin	- Limit access to administrator - Automation scans for changes to the system - implement a File access control policy - Access control policy(A.9.1.1) - Information access restriction(A.9.4.1) - Secure log-on procedures(A.9.4.2) - Access control to program source code(A.9.4.5) - Management of technical vulnerabilities(A.12.6.1) - Information transfer policies and procedures(A.13.2.1) - implementing information security continuity(A.17.1.2) - Protection of records(A.18.1.3)	Low	High	£10,000	Y	Low
13	(**Human**) The quality assurance person does not acknowledge a fraudulent product and has considered it to be a legitimate product.		**X**		IT Manger CEO	- Fraud training and education - Product line overseer	High	Med	£50,000	N	High
14	(**Hardware**) An attacker is able to obtain administrator privileges from the Extreme Networks X670V-48T by entering the administrator password conjoined with the 'service start-shell' CLI command within the shell.	**X**	**X**	**X**	Support Technician System admin Network admin	-Update OS and software - Threat detection installation - Management of technical vulnerabilities(A.12.6.1) - Network controls(A.13.1.1) - Security of network services(A.13.1.2)	High	High	£250,000	N	Very High

15	(**Hardware**) HPE PROLIANT ML350 GEN10 SERVER prone to a denial-of-service attack and compromise overall system integrity as well as breach of data due to a local bypasses security restrictions vulnerability.	**X**	**X**	**X**	Support Technician System admin Network admin	- Black listing IP addresses - Management of technical vulnerabilities(A.12.6.1) - Network controls(A.13.1.1) - Security of network service(A.13.1.2) - Segregation in networks(A.13.1.3) - Planning information security continuity(A.17.1.1) - implementing information security continuity(A.17.1.2) - Protection of records(A.18.1.3)	Low	High	£10,000	Y	Low
16	(**Software**) A XSS attack which targets the HPE PROLIANT ML350 GEN10 SERVER which hosts the web interface can lose confidential information.	**X**			Support Technician System admin	- Filter input on Arrival - Encode data on Output - Implement appropriate headers - Content security policy - Management of technical vulnerabilities(A.12.6.1) - Network controls(A.13.1.1) - Planning information security continuity(A.17.1.1) - implementing information security continuity(A.17.1.2)	Med	High	£50,000	N	High
17	(**Software**) Windows Server 2016 is vulnerable to remote executions when windows DB improperly handles objects within the memory which can affect its overall integrity and availability of accessing data.		**X**	**X**	Support Technician System admin	- Update OS and software - Equipment maintenance(A.11.2.4) - Management of technical vulnerabilities(A.12.6.1) - Network controls(A.13.1.1) - Security of network services(A.13.1.2)	Low	High	£10,000	Y	Very low
18	(**Business**) Organization not being ISO 27001 certified can display a weak security infrastructure and overall bad reputation.				CEO	- Build a certified ISMS system - Hire or find an information security officer (ISO) - Find a trusted certification body - Policies for information security(A.5.1.1) - Information security requirements analysis and specification(A.14.1.1) - Secure development policy(A.14.2.1) - Secure development environment(A.14.2.6) - Responsibilities and procedures(A.16.1.1)	Very High	Low	£10,000	Y	Med
19	(**Human**) Employees stealing and misusing consumer data for personal gain from the quality check process	**X**			IT Manger	- Product line overseer - Policies for information security(A.5.1.1) - Information security roles and responsibilities(A.6.1.1) - Management responsibility(A.7.2.1) - Information security awareness, education, and training(A.7.2.2) - Disciplinary process(A.7.2.3) - Termination or change of employment responsibilities(A.7.3.1) - Management of removable media(A.8.3.1) - Physical media transfer(A.8.3.4) - Access control policy(A.9.1.1) - User registration and de-registration(A.9.2.1) - User access provisioning(A.9.2.2) - Management of privileged access right(A.9.2.3) - Review of user access rights(A.9.2.5) - Removal or adjustment of access rights(A.9.2.6) - Information access restriction(A.9.4.1) Secure log-on procedures(A.9.4.2)	High	Med	£50,000	N	High
20	(**Hardware & software**) A rerouting attack that targets Extreme Networks X670V-48T , Amazon EC2 and AWS to obtain confidential consumer and employee data.	**X**			Support Technician System admin	-Implement a web application fire wall - Automated web scanners -Update OS and software - Threat detection installation - Controls against malware(A.12.2.1) - Network controls(A.13.1.1) - Security of network services(A.13.1.2)	Low	High	£10,000	Y	Very Low

					Network admin	- Segregation in networks(A.13.1.3) - Planning information security continuity(A.17.1.1) - implementing information security continuity(A.17.1.2)					
21	(**Software**) Fake AWS webform that redirects users to obtain confidential or personal consumer or employee data.	**X**			IT Manger Network admin	-Implement a web application fire wall - Automated web scanners -Update OS and software - Information access restriction(A.9.4.1) - Management of technical vulnerabilities(A.12.6.1) - Network controls(A.13.1.1) - Segregation in networks(A.13.1.3) - Information transfer policies and procedures(A.13.2.1) - Responsibilities and procedures(A.16.1.1) - Reporting information security weaknesses(A.16.1.3)	High	Med	£50,000	N	Very High
22	(**Human**) An ex-employee maintains or remembers security data and is able to gain unauthorised access to the premise or systems.	**X**	**X**	**X**	IT Manger Chief technician officer	- Introduce CCTV cameras around the premise. - Regularly update locks - revoke access rights and access credentials -Introduce remote monitoring - Disciplinary process(A.7.2.3) - Termination or change of employment responsibilities(A.7.3.1) - Information access restriction(A.9.4.1) - Physical security perimeter(A.11.1.1) - Physical entry controls(A.11.1.2) - Securing offices, rooms, and facilities(A.11.1.3) - Protecting against external and environmental threats(A.11.1.4) - Equipment siting and protection(A.11.2.1) - Security of equipment and assets off-premises(A.11.2.6) - Unattended user equipment(A.11.2.8)	High	Med	£50,000	N	High
23	(**Human & Data**) An employee being vulnerable to a shoulder surfing attack from another employee while looking at sensitive data.	**X**			IT Manger	- implement a privacy screen - Policies for information security(A.5.1.1) - Information security roles and responsibilities(A.6.1.1) - Terms and conditions of employment(A.7.1.2) - Information security awareness, education, and training(A.7.2.2) - Disciplinary process(A.7.2.3) - Termination or change of employment responsibilities(A.7.3.1) - Confidentiality or nondisclosure agreement(A.13.2.4) - Responsibilities and procedures(A.16.1.1) - Protection of records(A.18.1.3) - Privacy and protection of personally identifiable information(A.18.1.4)	High	Low	£25,000	N	Med
24	(**Human**) Products damaged / destroyed after being received from delivery due to inadequate handling.		**X**		IT Manger CEO	- Make sure products are securely attached - Carefully package products - Identify a route that doesn't cause damage due to obstacles - Working in secure areas(A.11.1.5) - Delivery and loading area(A.11.1.6) - Equipment siting and protection(A.11.2.1) - Monitoring and review of supplier services(A.15.2.1) - Managing changes to supplier services(A.15.2.2)	Very high	Low	£10,000	Y	Med
25	(**Hardware**) Database backup interrupted due to an environmental flood that has compromised the integrity and availability of the backup source.		**X**	**X**	System admin Network admin	- Implement back up emergency generators - Raise hardware above water level -Incorporate more than one backup source - Protecting against external and environmental threats(A.11.1.4)	Med	Med	£10,000	Y	Low

					Chief technician officer						
26	(**Human & software**) Phishing email attack which when opened by an employee deploys a ransomware software which spreads and makes systems unavailable until the ransom is paid.		**X**	**X**	IT Manger System admin Network admin CEO	- Avoid using public networks - Use SSL credentials for verification - Avoid pop ups and attachment from unknown sources -Update OS and software - Information security awareness, education, and training(A.7.2.2) - Access to networks and network services(A.9.1.2) - Controls against malware(A.12.2.1) - Segregation in networks(A.13.1.3)	Med	High	£50,000	N	Very High

Risk treatment

Controls (**table 6.1**) these are some specific controls that are useful to mitigate risks. These were designed as they were not suggested within the Annex-A, and I felt that they would be relevant.

Table 6.1 - Controls

Control	Description	Risk ID's
Threat detection installation	Antimalware software and firewalls implemented to protect endpoints and gather information.	**3, 14, 20**
Implement multi-factor authentication	Implement multifactor authentication to provide strong security with the use of two or more ways of authenticating an employee.	**2, 8**
Social engineering prevention &training	Introducing prevention method to prevent the occurrence of social engineering attacks from working. Some prevention methods such as using anti-virus and the use of security tools.	**9**
Threat training and education	These are implemented training exercises which are designed to inform employees of the different type of threats that can occur as well as how to safely avoid and or mitigate them.	**9**
Fraud training and education	This is the use of training methods and exercises to inform employees on the different types of frau and how to identify fraudulent products.	**13**
Communication verification	When employees are communicating internally or externally, they must provide a verification ID or code to prove the legitimacy of both parties.	**5, 9**
Product line overseer	This is an individual who oversees the operation of employees making sure that nothing bad happens to both the employees and systems.	**13, 19,**
Blacklisting IP addresses	This is the process of filtering out illegitimate or malicious IP addresses from accessing networks. Blocking this address help's mitigate attacks.	**1, 15**
Automated scanning for weak passwords	Introduce and use an automated password scanner (such as nFront) to scan passwords stored within a directory and will identify any compromised or weak passwords and who it belong to.	**2**
Use prepared statements	This is a method coding designed to maintain security when accessing SQL databases. These statements are used to execute parameterized queries without the possibility of an SQL injection.	**3**
Use stored procedure	This is an SQL statement that uses assigned names to form parameterised queries. This stored SQL code outside of the application which restrict the access of it from threats.	**3, 10**
Perform input Validation	This is the process of testing the input received for verification that data has been correctly entered into an input field and that it meets the specific requirements.	**3**
Enforcing least privilege	This is a principle that determines access by enforcing minimal level of user's rights or clearance level that the employee has to perform their role.	**3**
Introduce CCTV cameras around the premise.	This is to introduce or add more security cameras around the facility to provide more coverage for monitoring and to maintain security.	**4, 22**
Regularly update locks	This is the process to change physical locks to the building by updating codes or physically changing the locking mechanism. This prevent threat agents from gaining access as well prevent ex-employee's from gaining access.	**4, 22**
Introduce remote monitoring	To implement and use devices or external companies that allow for the ability to monitor the physical perimeter of the facility from a remote location. (I.e., paid external security company, cameras & motion sensors).	**4, 22**
Implement a VPN	VPNs can be implemented to create a secure environment when using confidential information. These are typically implemented within a local network and use to encrypt to protection data.	**5**
Filter input on Arrival	This filters the input from user by removing controlled character to prevent detrimental command from being executed.	**6, 16**
Encode data on Output	This is the process where users' data being outputted is encoded to prevent it from being interpreted as active content.	**6, 16**
Implement appropriate headers	Implementing "Content-Type" headers which prevent XSS responses in HTTP.	**6, 16**
Content security policy	This policy adds a layer of security which helps detect and mitigate XSS attacks and impact of XSS vulnerabilities.	**6, 16**
Implement an instruction detection system	These are software applications that are designed to monitor networks for any malicious activity and directly notifies administrators if necessary. Designed to prevent an attack from happening.	**7**

Configure endpoints	This is the process of changing security configuration settings to help reduce the attack surface and reducing or blocking as much as possible without out affecting required functions.	**7**
IP whitelisting	This is when you grant network access to only a specific IP addresses. This is designed to reduce the attack surface.	**8**
Single sign-on	Single sign on is the process of authentication that enables users to securely authenticate themselves with the use of different devices and or resources however, using one set of credentials.	**8**
Spam Filter	These are software applications that identify unsolicited and unnecessary emails that may cause detrimental damage if opened.	**9**
Update OS and software	The simple process of updating any software being used as well as to check if your current Operating system needs updating.	**11, 14, 17, 20, 21, 26**
Limit access to administrator	This is simply making sure that only administrators have access to critical systems only and they users will need to talk to them in order to make changes to the system.	**12**
Automation scans for changes to the system	This is software that scans files and directory for any recent changes it is designed to verify the integrity of data stored to previous backups making sure data is correct.	**12**
implement a File access control policy	This is an access control process which determines what file / data certain employees can access depending on their level.	**12**
Build a certified ISMS system	This is a system that defines and manages a business to implement a secure process of protecting the confidentiality, integrity, and availability of assets.	**18**
Hire or find an information security officer (ISO)	This can be someone internally or externally hired and is responsible for establishing and maintaining information assets and critical systems are protected.	**18**
Find a trusted certification body	These are organisations that provide assessments based around the standard the business wants. Once achieved the body will award the business with a certificate to show they are certified.	**18**
Implement a web application fire wall	An application that detects malicious activity by monitoring the network traffic and redirects any threat agents from your site. It also	**20, 21**
Automated web scanners	These scanner perform daily and regular scan independently to detect malware within the files and or database folder of your website. These scanner are able to remove any detrimental code if needed.	**20, 21**
Revoke access rights and access credentials	All credential and access rights should be revoked from ex-employees.	**22**
Implement a privacy screen	There are screen filters which prevent people from reading your computer screen from different angels. The screen scan only be read by directing looking at the screen.	**23**
Make sure products are securely attached	Before starting a delivery make sure packages are attached within the vehicle by using rope ties of secure compartments to prevent products from moving while in transit.	**24**
Identify a route that doesn't cause damage due to obstacles	Identify a route that doesn't cause damage to product due to obstacles such as potholes or sharp turns.	**24**
Carefully package products	Wrap product in materials to add additional layers of protection.	**24**
Implement back up emergency generators	These are a set of generators that are stored within a secure location which are designed to be used if the main power source was to fail. This will allow for operations to continue.	**25**
Raise hardware above water level	This is to place hardware or selves or different levels of the building which would be above ground level to prevent hardware from being damaged by water.	**25**
Incorporate more than one backup source	Introduce multiple backup sources such as both digital clouds services and or physical devices that are placed externally from the building.	**25**
Avoid using public networks	Employees are devices should only be connected to local private network as public network can allow attackers to enter systems and or device using different attacks. Additionally public network do not offer as much protection as that of a private one.	**26**
Avoid pop ups and attachment from unknown sources	Any pop ups or attachments within emails should be avoid and discarded to prevent any malicious actions from taking place and compromising systems.	**26**
Use SSL credentials for verification	These are online certificates that are issued for specific domain to verify that they are legitimate and a safe to use. This also provides secure channels and connections.	**26**

Annex-A controls (**table 6.1**)is a list of implemented controls that can be found within the ISO 27001 2013. These controls are considered to be industry standard and ensure that the overall security of the business is maintained.

Table 6.2 - Annex A controls

Control		Description	Impl	Justification inclusion	Justification exclusion
A.5 Information security policies					
A.5.1 Management direction for information security					
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.					
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties	**Y**	Risks: 18,19,23	**X**
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	**Y**	This is a necessary control due customer data being an important aspect of Fizzit there will need	**X**

				policies to protect that data securely especially for new emerging threats.	
A.6 Organization of information security					
A.6.1 Internal organization					
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization					
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	**Y**	Risks: 8, 19, 23	**X**
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	**Y**	This can minimize human error as the workload is spread across numerous people. This also reduces attack spread and potential agents.	**X**
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	**Y**	This is important as being able to quickly contact authorities during an undesirable event can reduce any casualties and or damage.	**X**
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained	**N**	**X**	Company has no special interest groups or is part of a community of a larger organisation.
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	**Y**	Project management is important as it ensures what is being delivered is correct and that it provides opportunity for the business.	**X**
A.6.2 Mobile devices and teleworking					
Objective: To ensure the security of teleworking and use of mobile devices.					
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices	**Y**	Control used to maintain confidentiality of information between mobile channels is important especially has majority of employees will have one.	**X**
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites	**N**	**X**	No communication sites
A.7 Human resource security					
A.7.1 Prior to employment					
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.					
A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	**Y**	A necessary process the company should do before hiring individuals. This is to verify that they may not cause any problems.	**X**
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	**Y**	Risks: 8, 2	**X**
A.7.2 During employment					
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.					
A.7.2.1	Management responsibility	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization	**Y**	Risks: 19	**X**
A.7.2.2	Information security awareness, education, and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	**Y**	- Risks: 2, 6, 8, 19, 21, 23, 26 - GDPR and training and awareness	**X**
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to act against	**Y**	Risks: 8, 19, 22, 23	**X**

		employees who have committed an information security breach.			
A.7.3 Termination and change of employment					
Objective: To protect the organization's interests as part of the process of changing or terminating employment.					
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.	**Y**	Risks: 8, 19, 22, 23	**X**
A.8 Asset management					
A.8.1 Responsibility for assets					
Objective: To identify organizational assets and define appropriate protection responsibilities.					
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	**Y**	This helps organise and manage assets as well as making sure assets don't go missing.	**X**
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned	**N**	**X**	Not necessary process as multiple employee use the same asset.
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented.	**Y**	A useful control used to help educate and inform on the correct practice within the workplace. To prevent accidents to both employees and assets.	**X**
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract, or agreement	**Y**	A necessary process for termination of employees.	**X**
A.8.2 Information classification					
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.					
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification	**Y**	A useful control to organise and manage data, making it easily indefinable and accessible.	**X**
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization	**Y**	A necessary component when A.8.2.1 is implemented	**X**
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization	**Y**	A necessary component when A.8.2.1 is implemented	**X**
A.8.3 Media handling					
Objective: To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.					
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization	**Y**	Risks: 19	**X**
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures	**N**	**X**	Not a relevant procedure of Fizzit
A.8.3.4	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation	**Y**	Risks: 19	**X**
A.9 Access control					
A.9.1 Business requirements of access control					
Objective: To limit access to information and information processing facilities.					
A.9.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and information security requirements.	**Y**	Risks: 4, 8, 12, 19, 22	**X**
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use	**Y**	Risks: 26	**X**
A.9.2 User access management					
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services					
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	**Y**	Risks: 4, 8, 19	**X**

A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	**Y**	- Risks: 8, 19 - GDPR	**X**
A.9.2.3	Management of privileged access right	The allocation and use of privileged access rights shall be restricted and controlled.	**Y**	A useful control to minimize unauthorised access.	**X**
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	**Y**	Useful control for maintaining confidential information.	**X**
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	**Y**	Useful for providing training and understanding of an employee's position when using assets.	**X**
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.	**Y**	Risks: 8, 19	**X**
A.9.3 User responsibilities					
Objective: To make users accountable for safeguarding their authentication information.					
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	**Y**	Risks: 2	**X**
A.9.4 System and application access control					
Objective: To prevent unauthorized access to systems and applications.					
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy	**Y**	Risks: 2, 8, 12, 19, 21, 22	**X**
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	**Y**	Risks: 2, 11, 12, 19	**X**
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords	**Y**	Risks: 2	**X**
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	**Y**	An important control due to companies' operation and use of different critical systems.	**X**
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	**Y**	Risks: 12	**X**
A.10 Cryptography					
A.10.1 Cryptographic controls					
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.					
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	**N**	**X**	Not necessary as company does not have cryptographic elements
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	**N**	**X**	Not necessary as company does not have cryptographic keys
A.11 Physical and environmental security					
A.11.1 Secure areas					
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities					
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	**Y**	Risks: 4, 11, 22	**X**
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	**Y**	Risks: 4, 22	**X**
A.11.1.3	Securing offices, rooms, and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	**Y**	Risks: 4, 22	**X**
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied	**Y**	Risks: 11, 22, 25	**X**

A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	**Y**	Risks: 24	**X**
A.11.1.6	Delivery and loading area	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access	**Y**	Risks: 24	**X**
A.11.2 Equipment					
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.					
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	**Y**	Risks: 4, 11, 22, 24	**X**
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	**Y**	A useful control for environmental threat agents.	**X**
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.	**Y**	A useful control for environmental threat agents as well as maintain information security and overall operation.	**X**
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	**Y**	Risks: 10, 17	**X**
A.11.2.5	Removal of assets	Equipment, information, or software shall not be taken off-site without prior authorization.	**Y**	A necessary control for maintaining security and minimizing theft.	**X**
A.11.2.6	Security of equipment and assets off-premises	Equipment, information, or software shall not be taken off-site without prior authorization.	**Y**	Risks: 22	**X**
A.11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	**Y**	A general control necessary to safely dispose of unnecessary assets.	**X**
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	**Y**	Risks: 4, 10, 11, 22	**X**
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted	**Y**	Used to maintain unauthorised access and to maintain confidentiality	**X**
A.12 Operations security					
A.12.1 Operational procedures and responsibilities					
Objective: To ensure correct and secure operations of information processing facilities.					
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them	**Y**	Provides a useful way of training employees of certain procedures if necessary	**X**
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	**Y**	This can be a useful way to uncover vulnerabilities or problems that were currently affecting the business and to change them.	**X**
A.12.2 Protection from malware					
Objective: To ensure that information and information processing facilities are protected against malware					
A.12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness	**Y**	Risks: 7, 10, 20, 26	**X**
A.12.4 Logging and monitoring					
Objective: To record events and generate evidence.					
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed	**Y**	1	**X**
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access	**Y**	Log information can be a used as evidence and must be kept safe and is also a legal requirement.	**X**
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged, and the logs protected and regularly reviewed	**Y**	Used control to gather evidence and maintain access control	**X**

A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	**N**	**X**	Not necessary control for Fizzit to introduce.
A.12.5 Control of operational software					
Objective: To ensure the integrity of operational systems.					
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	**Y**	Risks: 7	**X**
A.12.6 Technical vulnerability management					
Objective: To prevent exploitation of technical vulnerabilities.					
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	**Y**	Risks: 1, 3, 6, 7, 10, 11, 12, 14, 15, 16, 17, 21	**X**
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented	**Y**	Risks: 7	**X**
A.12.7 Information systems audit considerations					
Objective: To minimise the impact of audit activities on operational systems.					
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	**Y**	Audits ae a necessary component for verifying activity.	**X**
A.13 Communications security					
A.13.1 Network security management					
Objective: To ensure the protection of information in networks and its supporting information processing facilities.					
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	**Y**	Risks: 1, 3, 14, 15, 16, 17, 20, 21	**X**
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	**Y**	Risks: 3, 14, 15, 17, 20	**X**
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	**Y**	Risks: 1, 3, 11, 15, 20, 21, 26	**X**
A.13.2 Information transfer					
Objective: To maintain the security of information transferred within an organization and with any external entity.					
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities	**Y**	Risks: 5, 12, 21	**X**
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	**Y**	Risks: 5	**X**
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	**Y**	Risks: 15	**X**
A.13.2.4	Confidentiality or nondisclosure agreement	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented	**Y**	Risks: 8, 23	**X**
A.14 System acquisition, development, and maintenance					
A.14.1 Security requirements of information systems					
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.					
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	**Y**	Risks: 5, 18	**X**
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	**N**	**X**	Fizzit are not using a public network

A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	**Y**	This is a necessary control due to Fizzit sending and receiving money as part of their business model	**X**
A.14.2 Security in development and support processes					
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.					
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization	**Y**	Risks: 18	**X**
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	**N**	**X**	Fizzit are not in development process, so this control is unnecessary
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security	**N**	**X**	Fizzit are not in development process, so this control is unnecessary
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	**Y**	Risks: 6	**X**
A.14.2.5	Secure system engineering principle	Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts.	**Y**	Necessary control to record the events or any engineering for systems	**X**
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle	**Y**	Risks: 18	**X**
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	**N**	**X**	Fizzit do not need to monitor outsource development.
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	**Y**	A useful process to identify problems and uncover vulnerabilities	**X**
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new versions.	**Y**	A set of processes to see if system meets specified requirements	**X**
A.14.3 Test data					
Objective: To ensure the protection of data used for testing.					
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected, and controlled.	**N**	**X**	Fizzit do not have or need to protect test data
A.15 Supplier relationships					
A.15.1 Information security in supplier relationships					
Objective: To ensure protection of the organization's assets that is accessible by suppliers.					
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented	**N**	**X**	Fizzit do not have a supplier
A.15.1.2	Addressing security within supplier agreement	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	**N**	**X**	Fizzit do not have a supplier
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	**N**	**X**	Fizzit do not have a supplier
A.15.2 Supplier service delivery management					
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.					
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	**Y**	Risks: 24	**X**
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	**Y**	Risks: 24	**X**

A.16 Information security incident management					
A.16.1 Management of information security incidents and improvements					
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses					
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents	**Y**	Risks: 3, 18, 21, 23	**X**
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	**Y**	Risks: 3, 6	**X**
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	**Y**	Risks: 3, 20	**X**
A.16.1.4	Assessment of and decision on information security event	Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.	**Y**	Risks: 7	**X**
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures	**Y**	An important control that can help improve Fizzit response to incidents as well as for them to lessen the affects.	**X**
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	**Y**	A useful control that can provide education and training for employees of recent incidents.	**X**
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence	**Y**	A necessary process for that maybe required by legal authorities	**X**
A.17 Information security aspects of business continuity management					
A.17.1 Information security continuity					
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.					
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster	**Y**	Risks: 15, 16, 20	**X**
A.17.1.2	implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation.	**Y**	Risks: 7, 12, 15, 16, 20	**X**
A.17.1.3	Verify, review, and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	**Y**	The importance of understanding how to maintain information security in the event is important for Fizzit as it could allow for their operation to be unaffected	**X**
A.17.2 Redundancies					
Objective: To ensure availability of information processing facilities.					
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements	**N**	**X**	No processing facilities
A.18 Compliance					
A.18.1 Compliance with legal and contractual requirements					
Objective: To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.					
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organization.	**Y**	Legally it is mandatory to implement	**X**
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual	**Y**	Important to consider if there is anything that can be copied or stolen	**X**

		property rights and use of proprietary software products.			
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, contractual, and business requirements	**Y**	Maintaining the integrity of records is important and is a legal requirement	**X**
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	**Y**	Risks: 5, 6, 8, 23	**X**
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations.	**N**	**X**	Not necessary as company does not have cryptographic controls
A.18.2 Information security reviews					
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures					
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur	**Y**	It is important to review information security to understand its importance and to make sure it is legally suitable and that all components have been met	**X**
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.	**Y**	Compliance with information security policies and standards make sure Fizzit are meeting legal obligations.	**X**
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	**Y**	examination of operational systems to ensure that hardware and software controls have been correctly implemented	**X**

Security polices (**table 7.1**) are some recommendation of polices that should be considered for implementation and tailored more directly for Fizzit.

Table 7.1 - Security policies

Security policy	Description
Acceptable use Policy	This policy specify the restrictions and practices that an employee using IT assets must agree and understand in order to continue to access that particular asset. It should be a standard agreement that all new employees agree upon once starting.
Data breach response policy	This is a policy that has the sole purpose of describing the process of handling an incident and remediating the impact on the business operations.
Disaster recovery	This plan provides a detail process of how to manage different incidents that the business may face. This plan is activated when significant incident has impacted the business greatly.
Business continuity plan	This plan describes how the business will operate in the event of an undesired event typically works alongside the Disaster recovery plan with the overall goal to restore businesses operation and continuity of critical assets.
Remote access policy	This should be considered due to current climate with Covid-19. The implementation of remote access and work helps define the correct procedures with externally accessing internal systems or data. Providing security of different networks.
Access control policy	A standard policy which controls the access of different assets maintaining an organised process of authorisation. Providing an overall secure access process for delicate system and or data.

References

- **FIRST Forum of Incident Response and Security Teams**. 2015. *Common Vulnerability Scoring System Version 3.1 Calculator*. [online] Available at: <https://www.first.org/cvss/calculator/3.1> [Accessed 10 November 2021].
- **CVE Mitre.** 1999. *Search CVE list*. [online] Available at: <https://cve.mitre.org/cve/search_cve_list.html> [Accessed 10 November 2021].
- **2013. Information technology - Security techniques - Information security management systems - Requirements.** *[ebook]* Available at: <https://learn-eu-central-1-prod-fleet01-xythos.content.blackboardcdn.com/5d108c67a3df7/4953766?X-Blackboard-Expiration=1639591200000&X-Blackboard-Signature=cQtQEz%2F8kaIG3GIrD7rtRUEW5JOsIeoMeo1uwrzjN9U%3D&X-Blackboard-Client-Id=160649&response-cache-control=private%2C%20max-age%3D21600&response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27iso27001-2013.pdf&response-content-type=application%2Fpdf&X-Amz-Security-*Token=IQoJb3JpZ2luX2VjEIz%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaDGV1LWNlbnRyYWwtMSJGMEQCIB%2B%2BM1%2FreLaA6FKgJeiJchNsExFo4PvbuqZ31nDRBAizAiBwfAuM6WqWSM8gtC8TlkYcZIQ86900YO3t%2BMsMyqCjfSqABAh1EAIaDDYzNTU2NzkyNDE4MyIMKw9IrnMFdjR83MhzKt0DTnZCAg68Z%2Fs6DxASyXLdsZHjeGXADkX6FKH47i8O8FwgVI3SRUNLsS71aP41WO6oms5iGfXhs4PVYNEOCfQSGRJ%2FRHdrdx2vj5Ll244j9IEoNenutTp9Sv%2B59IHMs0Bk1I7A7MWoAMRkUfy87WZFVHle3aDBKBHJpX%2FyzVRWBLxdvxJ%2BAviNqkJHEFphOiBgmpSQQ2q8a8BGXa9DJMSUTj4gkjzW9%2BeW%2BOidTBiiwolnAcxU%2FDuy2j1Pw2Q%2B8l5Lwul1ZrDg3ljycSSaz%2FnotZcdXgEAlF92gw2kivVlapsGg8ZfGcKMe3TULqU%2Ff8Np7PFFaxEpLa7PMqcFZxsQeMx4Y1Qg7RCVWwITGvsM6X9RKjA9NhMiQFV%2B9Ew4u7%2Ft%2BWyB6dYUh5yBDaHPNUIuf6A7hmnVWAzSCStvHhvJ5mvGDltXK%2Bh3%2FAEDShJXDslMCSPlrlB1pnPm8WddERb4GvuU5%2BoR%2B0jzo1jWULhSiBkIKYm6vuc%2FT5Sb4RZmvH%2FEx265sGpN6n9Gk2U9Ogd9B9735Pcl7%2FMGJewhttlpqpq6BRXGkLQcR%2BXtXAuzGB4JUKIpO2MZLncXT846975z47gAV9bEP99ieuOltGn4NWxhcTE7xy0REe57kAaMMOen540GOqYBDboOpPj5rZLs04qY3ha%2B5ec8cvPZyxPK9TZ11jlV5IjdtrnhNYYym4QMD9wGixdkvk7mTyILnosaXukz8sAbLlXe3okeHnCKTuyO3LD%2FsEKYV9%2F68KQor2dBgpVHCFPyypwZe6XFrk5s0LSy1uwwkyHUTdBHQ3HAZnWr%2F9slD%2FJ1JNX5xNA7wJPBkcnx3Cpy%2FdnHxLfPnUPkiHVM5lZEE1JJ0mWFUA%3D%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20211215T120000Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=ASIAZH6WM4PL2TM7YM4Q%2F20211215%2Feu-central-1%2Fs3%2Faws4_request&X-Amz-Signature=ce7cf4119ebc18121e2840064f4c612cc3b613eab8d2f9064c1ac151101ee9a0> [Accessed 2 October 2021].*
- **Owasp.org. 2021. *Vulnerabilities* | *OWASP***. [online] Available at: <https://owasp.org/www-community/vulnerabilities/> [Accessed 16 November 2021].