CYBR373 - Assignment 1 - Risk Assessment
greenthom - 300536064

Task One: Rating and Classification Definitions

CIA Triad	Requirements
Confidentiality	Protection of sensitive information/data from being accessed or disclosed by unauthorized individuals[1].
Integrity	The protection of data from unauthorized modification or destruction[1].
Availability	The assurance of timely and reliable access to data and systems by authorized users[1].

Value	Description
Confidential	Used for the most sensitive corporate information that must be tightly controlled, even within the organization. It requires a greater level of protection [2]. Should only be accessed by those with Confidential Clearance.
Private	Used for information that can be viewed by internal employees, authorized contractors, and third parties. It requires less level of protection than confidentiality[2]. Internal data/information not meant for public disclosure. This information must be securely stored and accessed only by those with authorized private/internal clearance.
Public	Used for information that has been approved for public release or use. It requires proportionately less protection than Confidential and Private[2]. Can be distributed and freely used, reused, and redistributed as it is not sensitive.

Likelihood	Description
Certain	It is easy for a threat to exploit the vulnerability without high-level skills or resources. The threat occurs frequently. No current control in place to prevent or detect threats[3].
Highly probable	It is feasible for a threat to exploit the vulnerability with minimal skills or resources. The threat is likely to occur frequently. Current control is in place but unlikely to prevent or detect threats[3].
Possible	It is feasible for a threat to exploit the vulnerability with moderate skills or resources. The threat is possible to occur. Current control is in place and can prevent or detect threats[3].
Possible but unlikely	It is feasible for a threat to exploit the vulnerability but would require skills or resources for it to occur. The threat is unlikely to occur. Current control is in place and makes it unlikely for threats to occur[3].
Rarely	It is difficult for the threat to exploit the vulnerability. The threat is not expected to occur. Current control is in place and makes it not expected to occur through prevention and detection[3].

Impact	Description
Severe	The company suffers severe corporate and public damage that is not easy to recover from. There is a loss of life public and/or staff.

	There is a severe H/S incident involving the public and/or staff. Legal liabilities and/or breach of SLAs. Severe economic loss. Severe risk impacting company objectives, service delivery, and productivity. The impact cannot be managed without external funding. Communications and recovery must be shared with customers/stakeholders. Disruption of operations requires severe recovery efforts.
Significant	The company suffers significant corporate and public damage. There is a significant H/S incident involving the public and/or staff. Significant economic loss. Potential legal liabilities and/or of SLAs. Significant risk impacting company objectives, service delivery, and productivity. The impact cannot be managed without external funding. Communications and recovery must be shared with customers/stakeholders. Disruption of operations requires severe recovery efforts.
Moderate	The company suffers limited corporate and public damage. There is a moderate H/S incident involving staff and/or a limited public. Moderate Economic loss. Possible legal liabilities and/or SLAs. Moderate risk impacting company objectives, service delivery, and productivity. The impact cannot be managed without re-planning some internal processes. Disruption of operations requires moderate recovery efforts.
Minor	The company suffers minor reputation damage from a corporate/public standpoint. There is a minor H/S incident involving a staff member or a member of the public. There is a minor economic loss. Minor legal liabilities and/or SLAs. Minor impact on company objectives, service delivery, and productivity. The impact can be managed within current resources, with some pre-planning.
Minimal	Reputation is not affected from a corporate/public standpoint. No loss or significant threat to health and safety involving staff and/or the public. There is no economic loss. Limited risk impacting company objectives, service delivery, and productivity. The impact can be managed with current resources and no re-planning. Minor disruption of operations, quick recovery.

Impact	Description
High 60-100	It will result in a loss of concern about EtherSpace's reputation with the public resulting in a large legal action or loss of assets impact on product delivery or cause EtherSpace significant revenue or earnings. Severe or catastrophic adverse effect on organizational operations, assets, or individuals.
Medium 30-60	It will result in a moderate loss of trust between EtherSpace and its customers or potential concern in legal action loss of some assets moderate impact on product delivery or cause EtherSpace to lose some revenue or earnings. Serious adverse effect on organizational operations assets or individuals.
Low 0-30	It will result in low reputational damage between EtherSpace and customers low impact on assets low impact on product delivery or little to no loss of revenue or earnings. Limited adverse effect on organizational operations, assets, or individuals.

Task Two: Asset identification and classification

ID	Asset Cat.	Asset	Employee Description/Attribute
001	Employees	CEO	**Role:** CEO **Description:** Owns and manages the company and is responsible for coordinating the day-to-day activities including issues of RFID access cards, managing financial data, hiring and termination of employees.

002	Employees	Engineers	**Role:** Engineer **Description:** Two engineers total who provide 24/7 support to customers through 12-hour shifts. They have full access to user account information. Other duties include**:** registering new users, activating and deactivating user accounts, deleting user accounts and data, backup, system maintenance/upgrades, and password reset. Also responsible for ensuring hardware components work properly, managing electrical systems within the data center, wiring, cooling systems, etc.

ID	Asset Cat.	Asset Name	Hardware Description/Attribute
003	Hardware	Network Attached Storage (NAS)	**Description:** Network-attached storage makes data continuously available for employees to collaborate effectively over a network. It is located in the office supply room. **Quantity:** 1 **Category:** Network Storage Backup
004	Hardware	Smoke Detector	**Description:** The smoke Detector is located in the break room. Off-shelf battery-powered smoke detectors installed (2 in EtherSpace main office and 2 in server room). **Quantity:** 4 **Category:** Safety devices
005	Hardware	Servers	**Description:** Servers storing customer data/information, services (VPS). **Quantity:** 24 **Category:** Systems
006	Hardware	WebM Server	**Description:** Server storing VPS management interface service (WebM). **Quantity:** 1 **Category:** Systems
007	Hardware	Port Switches	**Description:** Links devices on a network by receiving and forwarding data to the destination device. Establishes and maintains network structure. **Quantity:** 11 **Category:** Network device
008	Hardware	Routers	**Description:** Reads packets to determine where it is going, then forwards the packet to the destination. Establishes and maintains network structure. **Quantity:** 3 **Category:** Network device
009	Hardware	Air conditioning System	**Description:** Provides and maintains airflow in the server room. **Quantity:** 1

			Category: Safety device
010	Hardware	Power Distribution Module	**Description:** Switches power to different areas of the servers. **Quantity:** 2 **Category:** System
011	Hardware	Data Link	**Description:** Transmits data between different parts of a network or between networks. Runs at 10gbps. **Quantity:** 1 **Category:** Network device
012	Hardware	Desktop PC's	**Description:** Each engineer is assigned a dedicated desktop PC. CEO also has a dedicated desktop PC. **Quantity:** 3 **Category:** Systems
013	Hardware	Access Cards	**Description:** Provides access to rooms on the premise that the employees have authorized access too. **Quantity:** 3 **Category:** Systems, devices
014	Hardware	Safe	**Description:** Store company documentation, e.g. employee information. **Quantity:** 1 **Category:** Security Device

ID	Asset Cat.	Asset Name	Data Description/Attribute	Classification
015	Data	Customer Information	**Description:** All services are associated with the customer's number and registered email. **Owner:** EtherSpace	Confidential
016	Data	Transactional Information	**Description:** Transactional data including customer information; types of services purchased, full name, address, phone number, and email of customer, are saved in .csv format. Easily compatible through the use of other applications (e.g. Excel). **Owner:** EtherSpace	Confidential
017	Data	Data Backup Files	Description: All transactional data is located in the Network Attached Storage (NAS) drive. Backup occurs weekly on Friday at 11.30 pm. **Owner:** EtherSpace	Confidential
018	Data	Employment Documentation	**Description:** Employment documentation regarding EtherSpace employee information, personal and private. **Owner:** EtherSpace	Confidential

019	Data	RFID Access Control Logs	**Description:** Each provided RFID key has a unique identifier. The access control system logs each access (to the server room) and saves the information on the CEO’s desktop PC. **Owner:** EtherSpace	Confidential
020	Data	Customer VPS Information/ Data	**Description:** All customer data and operating system configuration on the VPS. **Owner:** Customer	Private
021	Data	Web and Service Information	**Description:** EtherSpace information and services is provided on the website. Service information (basic, advanced, premium, sub information) is provided too and stored by the domain management company. **Owner:** EtherSpace	Public

ID	Asset Cat.	Asset Name	Software Description/Attribute
022	Software	RFID Access Software	**Description:** RFID software was purchased from “Gaorfid” for $5000. Access is managed and tracked using the RFID key's unique identifier.
023	Software	Ubuntu Desktop	**Description:** All dedicated desktop PCs used by staff are running the latest version of Ubuntu Desktop.
024	Software	Firewall	**Description:** Protects against outside cyber attackers by shielding the network from malicious or unnecessary network traffic. Isolates internal subnet that manages internal devices.
025	Software	Email	**Description:** Use of email to communicate with customers. Provide account and service information to customers. Used to communicate with customers to reset or delete accounts.
026	Software	Hypervisor	**Description:** Software that you can use to run and create multiple virtual machines on a single physical machine. Every virtual machine has its operating system and applications. The hypervisor allocates the underlying physical computing resources such as CPU and memory to individual virtual machines as required.
027	Software	Debian 11 Linux Distribution	**Description:** Hypervisor software runs using Desbian 6 Linux distribution.
028	Software	Management Interface	**Description:** Web-based interface where customers are granted access to modify major aspects of their VPS service (e.g. change OS). Allows customers to reset their VPS to the initial state. Change the operating system, shut down, reboot. Allows customers to cancel their service immediately, where they will be presented with a confirmation link. User accounts and data are deleted immediately. The management interface is run by the WebM server.

029	Software	OpenOffice	**Description:** Provides office productivity tools. Open-source software. Provides applications/software for work.
030	Software	Customer Management Software	**Description:** Manages the customers and services they have paid for.
031	Software	SSH	**Description:** Allows remote access. Network protocol for using VPS services securely. Allows customers to log in to their VPS system using the account information that was emailed.
032	Software	Employee Access Control	**Description:** Staff have full access to Desktop PC's. This includes information/data that they have authorized access to. Have access to applications installed on desktop PC.
033	Software	Server Software	**Description:** Software on the servers used. These servers host VPS services and customer's data/information. Each server can support up to 20 virtual servers. Servers are managed through the hypervisor. All servers are located in the DMZ. Can be connected to any port.
034	Software	Virtual Servers	**Description:** Virtual servers are the VPS the customers have purchased. Created and managed through hypervisor.
035	Software	DMZ	**Description:** DMZ configuration includes network management and security software that handles access control and monitoring between the internal network and external networks. All servers (customer and WebM) and devices are located in the DMZ. All ports to and from the DMZ (to customer servers) are open for customers (i.e. clients).
036	Software	Intelligent airflow	**Description:** Software for the hardware in the server room. Directs air in the server room that has high temperature.

ID	Asset Cat.	Asset Name	Procedure Description/Attribute
037	Procedure	Customer Purchase Policy for Services	**Description:** All purchases of EtherSpace's services are made online through an external system (i.e. Google Pay). No credit card information is stored/saved locally or disclosed to EtherSpace employees. **Purpose:** Is for all services are activated once payments have been successfully processed and validated. Ensures that payment has been made, no income loss, no customer payment information is saved, and services aren't being issued to non-paying customers.
038	Procedure	Web Server Policy	**Description:** Web hosting is outsourced to be run by the external website and domain management company. Located externally. The company guarantees 99.99 percent uptime.

			Purpose: This is for engineers to not be involved or maintain the company website, so their duties are prioritized on focusing on internal customer, server, and hardware management and maintenance. The management company also specializes in web and domain management so they would be a better fit for maintaining and ensuring that Ethernet's website is available to the public.
039	Procedure	Data Backup Information Policy	**Description:** All transactional data, including customer information, is backed up to Network Attached Storage (NAS) drive. Backup occurs weekly on Friday at 11.30 pm. **Purpose:** To keep relevant customer information saved on Drive. Protects the integrity of the organization, and records customer information. Ensures availability, integrity, and recovery.
040	Procedure	Physical Access Control Policy	**Description:** All employees must use RFID keys to access onsite areas. This includes an office supply room, server room, and own office. Engineers do not have access to each other's rooms or the CEO's room. All employees are advised to shut the office supply room door after each access. If the door is not properly shut, the access system will beep after an hour. **Purpose:** This is to keep the contents of office rooms secure, and only grant access to authorized internal employees with issued RFID cards. Ensure restricted, secure access to sensitive areas and mitigations if rooms are not secure (access system beeps after one hour).
041	Procedure	Server Room Access Control Policy	**Description:** Employees have full access to all sections of the server room. Access is managed and tracked through the use of RFID keys given to each employee. **Purpose:** This is to keep the contents of the server room secure, and only grant access to authorized internal employees with issued RFID cards. Ensure restricted, secure access to sensitive areas and log employee entry to monitor granted access.
042	Procedure	Customer Information/ Access Policy	**Description:** Account information is emailed to the customer after the initial installation and setup of services. This includes how to access their respective VPS service and Management Interface credentials. **Purpose:** This is for newly created accounts; account holders can access their system. Protects integrity and availability of their data and access to their system. Once VPS services are set up and assigned, customers have full control over the system e.g. creation of user accounts. Provides login info to their unique system using SSH.
043	Procedure	Use of Personal Devices for Work Policy	**Description:** Engineers are advised to avoid using their laptops/devices to perform daily tasks. **Purpose:** This is to avoid the risk of information/data being kept on an external non-internally controlled device. Protect data against malicious software on a device that has not been recognized. Maintain confidentiality and integrity of data. Ensure information and data are used with computing resources within the organization.
044	Procedure	Operating System Update Policy	**Description:** All dedicated PCs used by staff must run the latest version of OS (Ubuntu Desktop). This is updated automatically.

			Purpose: This is to ensure that all company desktop PCs are up-to-date with the latest security patches. Ensure company information/data is protected.
045	Procedure	Internal Devices Security Policy	**Description:** All internal devices on the network including Desktop PCs and Network Attached Storage, are located within an internal subnet. This is isolated/protected by a firewall. **Purpose:** To protect company internal devices by isolating them within a secured subnet and firewall. The procedure maintains confidentiality, integrity, and availability of internal systems and data access.
046	Procedure	Management Interface and VPS Access Policy.	**Description:** Customers have full virtual control over their respective VPS system and Management interface once services are set up and assigned. Control of the VPS system includes the creation of user accounts within the VPS, installation of software, drivers, etc. The management interface allows the customer to modify aspects of their VPS service. **Purpose:** This is to provide customers control over their service and ensure access through providing credentials. Avoid the risk of information/modification of their system. Ensures availability, integrity, and confidentiality.
047	Procedure	Reset of Customer's VPS Procedure	**Description:** Customers can reset the VPS on the management interface which allows customers to reset the VPS to the initial state. Resetting the system to its initial state takes 5 minutes. All customer data and OS configurations are deleted in the process. Reset can also be carried out by phone or email to EtherSpace where they supply personal and service information to reset VPS management system passwords. **Purpose:** This is to ensure customers have full control over how they interact with their purchased system. Also protects against tampering from external third parties as they need access to either the management interface or provide personal/service information. Provides confidentiality, integrity, and availability.
048	Procedure	Customer Cancelling VPS Procedure	**Description:** Customer can use the VPS management interface to cancel their service. They will be presented with a confirmation link. If the user wants to cancel their service, all user accounts and data are immediately deleted. **Purpose:** This is to ensure customers have full control over their subscriptions and paid services. Ensures confidentiality, integrity, and availability.
049	Procedure	Customer Password Reset Procedure	**Description:** Customers can request a reset for their VPS management interface password by emailing or calling EtherSpace. To request password reset they will need to provide personal and service information. Engineers are not authorized to reset root account passwords. **Purpose:** This is to manage password resets securely. Ensures authorized personnel are the only ones able to make changes to the account. Ensures account integrity.
050	Procedure	Employment Documentation Policy.	**Description:** Employment documentation is kept in the safe. This safe is locked in the CEO's office. Only accessible by the CEO, with other employees unable to access when locked. **Purpose:** To maintain confidentiality and integrity of employee information. Safeguard sensitive information and ensure the CEO's office remains secure from unauthorized personnel.

051	Procedure	Employee Wireless Access and Password Control Policy	**Description:** Engineers are expected to use strong passwords for their devices as enforced by the data center. The data center does not provide wireless access to its employees for security reasons. **Purpose:** This is to ensure that no one unauthorized can access an individual's PC and access private/confidential information. Protect assets against viruses or malicious software. Maintain confidentiality and integrity of data.
052	Procedure	Service Sales Policy	**Description:** Sales of EtherSpace's services are exclusively handled through the website, with no internal or external counter sales allowed **Purpose:** To ensure sales processes are maintained through the use of external services and prevent unauthorized or untracked transactions.
053	Procedure	Data Monitoring Policy	**Description:** EtherSpace does not monitor customer data or software on their VPS. **Purpose:** To respect customer privacy and ensure that EtherSpace does not interfere with and/or track customer data.
054	Procedure	External Contractor's Physical Access Policy	**Description:** Office maintenance (e.g. plumbing, cleaning) is managed by external contractors. Temporary access is so physical access to premises can be allowed. **Purpose:** To maintain confidentiality and integrity of information. Ensure protection against malicious actors.

Task Three: Risk assessment worksheet, including threat vulnerability assessment

Likelihood of Occurrence is the probability that a specific vulnerability within EtherSpace will occur. **The impact** is the consequence of an event if it occurs. **Risk Rating** is the point where the likelihood and impact ratings intersect.

Impact	Severe	15	19	22	24	25
	Significant	10	14	18	21	23
	Moderate	6	9	13	17	20
	Minor	3	5	8	12	16
	Minimal	1	2	4	7	11
		Rarely	Possible but unlikely	Possible	Highly probable	Certain
		Likelihood				

ID	Asset ID	Threat	Vulnerability	Risk Description	Consequence	Impact	Likelihood	Risk Rating
R01	001, 002	Theft	There is no screening, monitoring, or logging process for employees entering the company premises.	This allows a disgruntled employee to steal the asset.	Economic loss. Disruption of business operations.	Severe	Highly Probable	24
R02		Theft	There is no screening, monitoring, or logging for employees entering the company.	This allows an outsider to enter the premises and steal the asset	Economic loss. Loss of confidentiality. Disruption of business operations.	Severe	Possible but unlikely	19
R03	004	Fire	Lack of adequate fire detection and suppression system	A fire could potentially start and reach all sections of the building	Loss of life. Legal liabilities as a result of loss of life. Disruption of business. Economic Loss.	Severe	Possible	22
R04	020, 034 037	External Service Disruption	External payment system (i.e. Google Pay)	External payment systems could be facing downtime or be undergoing cyberattacks. Existing/new customers are unable to make purchases via an external payment system due to unforeseen downtime.	Economic loss. Disruption of business operations. Operational Disruptions.	Significant	Possible but unlikely	14
R05	038, 021	External Service Disruption	External Web Hosting and Domain Management Company	External payment systems could be facing downtime or be undergoing cyberattacks, leading to the unavailability of web services. This would prevent users from accessing the company website.	Economic loss. Disruption of business operations.	Significant	Possible but unlikely	14
R06	039, 015 016, 017 003	NAS Backup Failure	Lack of safeguards and procedures if data handling of backup failure occurs.	Failures in the automated backup process or issues with the NAS drive could result in incomplete or corrupted backup data.	Data Loss. Operational Disruptions.	Significant	Possible	18
R07	040, 041	Weak Access Controls	Lack of protected physical access safeguards to secure areas.	Inadequate access controls and security measures for confidential areas. Allows disgruntled employees to gain access to confidential areas.	Data Loss. Loss of Confidentiality. Disruption of business.	Significant	Possible	18

R08	001, 002 048, 049 015, 020 025, 028	Phishing Attack	Weak and insufficient email security measures. Lack of employee awareness.	Employees may be targeted by phishing attacks, where attackers are impersonating customers into disclosing personal details.	Loss of Confidentiality. Disruption of business operations. Data Breach.	Significant	Possible	18
R09	037, 042 047, 015 016, 020 025, 028	Phishing Attack	Weak and insufficient email security measures. Lack of customer awareness.	Customers may be targeted by phishing attacks, where attackers are impersonating the company into disclosing EtherSpace credentials.	Loss of Confidentiality Disruption of Business. Data Breach.	Significant	Highly Probable	21
R10	022, 024 025, 028 030, 032 033, 034	Denial-of-Service	Lack of network defenses leading to exploitation of company online services.	DoS attack overwhelms network infrastructure with traffic, disrupting VPS services, and internal devices.	Service outage. Disruption of Business.	Severe	Possible	22
R11	024, 033 034, 045 005, 006 007, 008	Firewall Configuration	Lack of network firewall and port rules resulting in exposure of internal network.	All ports open between DMZ and the internal network for customer connections. Misconfiguration in firewall settings allows unrestricted port access exposing internal network and servers.	Disruption of Business. Data Breach. Data Loss. Attack Exposure.	Severe	Highly Probable	24
R12	002, 050 051, 053 016, 020	Insufficient Employee Screening	Lack of Background Checks.	Employees are trusted without background checks, increasing the risk of internal threats. This can lead to a potential for insider threats resulting in data breaches and operational issues.	Data Breach. Data Loss. Loss of Confidentiality. Disruption of Business.	Severe	Highly Probable	24
R13	042, 020 031, 034	SSH Access Vulnerabilities	SSH Service allows Root Access with Potentially Weak Authentication	Vulnerabilities in SSH configurations OR weak authentication allow unauthorized access to customer VPS instances.	Data Breach. Data Loss. Service Disruption.	Significant	Highly Probable	21
R15	002, 042 047, 048 049, 015 016, 020 028	Operation Incident/ Accident	Lack of procedure or handling of physical or logical assets, resulting in error or failure.	In-proper process carrying out registration and activation of new users. Failure to follow procedure when handling sensitive data.	Loss of confidentiality. Disruption of business operations.	Moderate	Possible	13
R16	001, 002 051, 030	Operation Incident/ Accident	Lack of procedure or handling of physical or logical assets, resulting in error or failure.	An employee uses a weak password for workstations, interfaces, or customer management software.	Data Loss. Loss of Confidentialities. Legal Liabilities.	Moderate	Possible but unlikely	9

R17	004, 005 009, 010	Technical Obsolescence	Lack of company safeguards, processes, and procedures to maintain assets.	Assets such as Fire alarms, air conditioning units, and office services are not maintained or checked	Service Interruption. Data Loss. Legal Liabilities Loss of Life.	Significant	Certain	23

Task Four: Current and Proposed control strategy for each vulnerability/threat/risk, residual risk, and escalation path.

ID	Existing Safeguards	Recommended Controls	Res. Risk
R12	1. Employees have RFID keys to access their office, supply room, and server room. 2. Engineers use a strong password policy on the dedicated PC assigned to them. 3. Engineers do not have access to each other's rooms or the CEO's office. 4. If the office supply room door is left open, the RFID system triggers an alarm after one hour.	The primary safeguard missing is background checks, which are not performed for employees at EtherSpace. I would recommend that employment tests and checks are carried out upon hiring an employee. Employee checks are already laid out by Employment New Zealand regulations. Checks can include criminal or credit history, and drug and alcohol testing [4].	13
R11	1. Uses a firewall to isolate internal devices from external networks. 2. Servers are located in a DMZ, which is a separate network segment designed to expose only necessary services to external networks. 4. All ports to and from DMZ are open to customer connections which allows clients to connect to their VPS servers using any service and port.	Open ports to servers are not necessarily deemed as a security risk, however, if they are vulnerable or misconfigured then services in conjunction with open ports can be used by malicious outsiders to move laterally across a network and gain access to company data[5]. Solutions are 1. Close unused/unnecessary ports to limit and reduce potential entry points for attackers[6]. 2. Regularly update OS for the latest security patches that make ports more resistant against known vulnerabilities[6]. 3. Whitelist ports so only specific ports in the firewall for client VPS connection are needed for their service.	19
R01	1. All employees have RFID keys to access their own office, office supply room, and server room. Each key has a unique identifier that is logged and tracked using an RFID system. 2. Engineers do not have access to each other's rooms or the CEO's room. 3. The RFID access system logs all access events and saves this information to the CEO's PC.	As discussed in R12 recommended controls, implementing background checks is performed during the job application process. Background checks into theft or other misdemeanors would give insight into past employee behavior [7]. No screening, or logging process for physical entry to company premises. Implementing the use of CCTV cameras at the company premises will ensure the safety of internal assets, and employees and protection from external actors.	18

R17	No existing processes or procedures regarding regular maintenance and checking of physical assets such as smoke detectors, air conditioning units, and other critical infrastructure.	There are battery-powered smoke detectors installed, however there is no mention of regular testing or maintenance. For smoke detectors, testing is meant to occur every month, and every six months vacuuming and dusting smoke alarms is recommended[8]. The performance of servers and operating systems is dependent on air-conditioning, so regular maintenance checks concerning the system's air filters, mechanical items, refrigerant levels, compressors, and electrical testing[9], should be added to company procedures for effective infrastructure operations.	14
R03	Off-shelf battery-powered smoke detectors installed in Etherspace. Two in the Etherspace main office and two in the server room. Intelligent Airflow in the server room to direct cooler air to areas in the server room that are overheating.	Etherspace does not have a Fire Safety, Evacuation Procedure, and Evacuation scheme [10] plan, which is integral for any workplace. In section 10 of the scheme[11], the owner "must have reasonable fire prevent precautions concerning (a) electrical wiring, equipment, and appliances, including portable electrical equipment and appliances". Due to the server room having a reasonable amount of electrical equipment and wiring, safety processes in case of fire or overheating of applications need to be set. Implementing sprinkler systems, fire extinguishers, and Fire Risk Assessments for all hardware and internal assets in Etherspace should be a priority to mitigate this risk.	18
R10	1. All internal devices, including Desktop PCs and Network Attached Storage (NAS), are located within an internal subnet isolated by a firewall. This helps prevent unauthorized external access. 2. All ports to and from the DMZ are open to clients to access their respective VPS services.	1. Using external providers and services that offer DoS and DDoS (i.e. Cloudflare, AWS) protection and ensure that the availability and performance of Etherspace systems, and the ability to mitigate an incoming threat. 2. Implementing incident response procedures and plan for DoS attacks will minimize service disruption. This procedure and plan will have steps for detecting, mitigating, and recovering from DoS attacks.	18
R09	No existing processes or procedures regarding customer phishing mitigations.	1. Letting clients know about the risks that phishing attacks pose and remind them that certain customer information will never be asked over email[12]. 2. Identification or indication that this email is "from Etherspace" such as a company logo or disclaimer at the bottom of the email, so the customer can have confidence that this email is indeed from Etherspace. 3. Implement customer reporting so that customers have an email address or online page to fill out if they receive an email posing as Etherspace that is deemed malicious. This will allow Etherspace to contact other customers to make them aware of potential attacks.	14
R13	Customers can access their VPS instances using SSH with root privileges. Root credentials are provided in emails sent to customers after services have been effectively set up. Customers are prompted to change their password for user root after logging in for the first time, so their service is secure.	Due to all ports being open for customer access to the VM, SSH using the root account is vulnerable to bots scanning the internet. Restriction and disabling of SSH root access for VPS access after initial VPS login will be vital to protect high-privilege users such as root. SSH to VPS service should involve the creation of user accounts for customers to log in as their respective user that has low permissions, and then switch to root users once in VPS. This would ensure customers data integrity and availability of their system.	14
R02	No existing processes, procedures, or controls regarding unauthorized entry by an outsider or member of the public.	No screening, or logging process for physical entry to company premises. Implementing the use of CCTV cameras at the company premises will ensure the safety of internal assets, and employees and protection from external actors.	9

R06	1. Transactional data, including customer information, is saved every Friday at 11:30 PM on the NAS drive. 2. Data is stored on a NAS drive located in the office supply room. 3. All employees have RFID keys to access the office supply room, so authorized physical access is needed to access the NAS drive preventing unauthorized tampering.	The backup procedure is highlighted (Asset 005) however this plan does not discuss backup failure or disaster recovery. Implementing failure and disaster procedures and steps is vital for company data integrity. Implementing regular backup testing and integrity checks will ensure that transactional data is complete and not corrupted. Implementing redundancy with the use of multiple backup methods would provide safeguards if data were not recoverable from NAS backup.	9
R07	1. All employees have RFID keys to access their own office, office supply room, and server room. Engineers don't have access to each other's room or the CEO's room. 2. Employees are advised to shut the office supply room after each access and if not shut properly access system will beep after an hour. 3. All employees have full physical access to all sections of the server room. The access is managed and tracked using the RFID keys given to each employee. 4. RFID keys have a unique identifier that logs each access and saves the information on the CEO's desktop PC.	The access system only beeps after one hour for the office supply room if not shut properly, this should be the case for the server room to increase physical security. Access to the server room is the only room that is tracked by the RFID. Access to the office supply room should also be tracked due to it holding vital assets/data (e.g. NAS drive). Implementing these existing components to multiple rooms will mitigate physical access vulnerabilities.	9
R08	No existing processes or procedures regarding employee phishing mitigations.	Implement the use of external anti-phishing software that is designed to detect/identify phishing content contained in emails and block the content. This will limit the risks of employees being exposed to active phishing content in emails. However, most software's do allow users the choice to be presented with the content regardless, so training employees on email security to effectively identify phishing emails will be essential to protect business operations.	10
R04	No existing processes or procedures regarding external payment system downtime mitigations.	If the external provider is facing downtime, EtherSpace should have an incident response plan highlighting the procedures and processes that it should take. Communication with current customers and new potential customers is key for business continuity. This should involve emails sent to existing customers, and banner head updates on the company website (to let potential customers be aware of the current situation). Communication and discussions of SLAs with external payment provider if they are facing downtime, so Etherspace can communicate with customers. This is necessary to reduce the impact of payment downtime on the business.	9
R05	Outsources web hosting and domain management to a specialized company that guarantees 99.99% uptime. This implies reliance on their expertise and	Implementing an incident response plan, if the external company is facing downtime. This will contain procedures and processes of communication and discussions of SLAs with external web/domain provider if they are facing downtime, so they can communicate the correct information with	9

	infrastructure. Based on the SLAs that the company provides which are uptime guarantees this shows they have good infrastructure put in place to manage possible risks and attacks.	customers. Communication with current and potential customers either through email or social media is vital to reduce the impact of downtime and maintain business operations.	
R15	1. Engineers have specific responsibilities including registering new users, activating or deactivating user accounts, handling backups, and system maintenance. Responsibilities are laid out and have clearly defined processes linked to them. 2. RFID access to specific areas with logs. This helps track physical access and ensures that only authorized personnel are handling sensitive data and processes.	Implementing performance and awareness training for new or existing employees. This will help improve employees' performance and prepare them to cover their roles. Will identify the training needs of both the company and the employee. This will provide employees with the importance of following laid-out procedures and handling sensitive data correctly. Also implementing and teaching employees incident response plan for handling errors or failures in processes so efficient recovery and communication steps are taken.	5
R16	1. Engineers are required to use strong passwords for their devices, including desktop PCs, reducing the risk of unauthorized access and potential security breaches. 2. All PCs used by staff are running the latest version of Ubuntu which is set to update automatically, ensuring new security patches and reducing vulnerability.	1. There is a password policy already in place, however, it is 'expected' of them to uphold this policy themselves. Enforcing policy requirements such as password complexity, regular password updates, minimum password length, etc., would provide extra security. This would also mean that employees have to conform to this policy and ensure they are using good password practices to achieve security across company systems. 2. Implementing security training for employees that covers the importance of password security and best practices will provide mitigation to this risk.	6

Escalation Matrix

CEO: Red (22-25), Orange(14-21).
Engineer: Yellow (4-13), Green(1-3).

Critical	Critical	Urgent	Important
Critical	Urgent	Important	Normal
Urgent	Important	Normal	Normal
Important	Normal	Normal	Normal

References

[1] What is the CIA Triad by Sangfor Technologies: https://www.sangfor.com/glossary/cybersecurity/what-is-cia-triad

[2] CYBR373 – Governance, Risk and Compliance Lecture Slides: https://ecs.wgtn.ac.nz/foswiki/pub/Courses/CYBR373_2024T2/LectureSchedule/W2-1.pdf

[3] Internal Affairs (New Zealand Government) - Risk Assessment Process (Resource used for Tutorial 1): https://www.digital.govt.nz/assets/Documents/3Risk-Assessment-Process-Information-Security.pdf

[4] Govt NZ Employment hiring techniques: **https://www.employment.govt.nz/starting-employment/hiring/tests-and-checks**

[5] Blog on open port vulnerabilities: **https://www.bitsight.com/blog/open-port-vulnerabilities-whats-the-big-deal**

[6] NordVPN on what are open ports: **https://nordvpn.com/blog/what-are-open-ports/#:~:text=Open%20ports%20by%20themselves%20do,gain%20control%20of%20the%20system.**

[7] Ministry of Justice - Criminal Records Employment Check: **https://www.justice.govt.nz/criminal-records/**

[8] Fire and Emergency NZ - Smoke Alarms: **https://www.fireandemergency.nz/home-fire-safety/smoke-alarms/**

[9] Computer Room Air Flow Best Practices: **https://blog.eecnet.com/eecnetcom/bid/91250/Computer-Room-Air-Conditioning-Maintenance-and-Best-Practices**

[10] Fire Safety and Evacuation Regulations 2018: **https://www.legislation.govt.nz/regulation/public/2018/0096/18.0/LMS46332.html**

[11] Fire Safety and Evacuation Regulations 2018 - Appliances: **https://www.legislation.govt.nz/regulation/public/2018/0096/18.0/LMS46379.html**

[12] Customer awareness for phishing emails: **https://sqnbankingsystems.com/blog/steps-to-take-when-customers-receive-phishing-emails/#:~:text=Let%20your%20customers%20know%20about,online%20passwords%20or%20ATM%20PINs.**