

Assignment 1: Risk Assessment

Due Date: 12/8/2024, at 23:59

Weight: 30% of overall grade for the course

This is an individual assignment

What to submit:

- Please submit a document (preferably a pdf file) containing answers to the tasks in the assignment.
- The tasks must be answered in the order of the assignment. (a, b, c, d, ...)
- Please state the course code and your name on the document header
- Maximum page limit is **12 pages** (*excluding* the cover page and Reference list)
- Diagrams (if any) must be included in the document file
- Plagiarism will be dealt with under the University policies and “copy and paste” answers will receive significantly lower marks than one you have written in your own words.
- Please disclose any use of generative AI (e.g., for brainstorming or editing) in the completion of this assignment.

Case Study: EtherSpace

EtherSpace is a small sized data centre which provides virtual, shared and dedicated Private Servers (VPS) to consumers in New Zealand. The data centre is located at Wellington Central Business District (CBD) on floor 1 of 12 Customhouse Quay Street. The company relocated to the new data centre 2 years ago. Businesses located in Wellington contribute to a large portion of EtherSpace's customers at the moment.

Organisational Structure and Roles

The company has the following structure and numbers indicate the number of staff for a specific job.

- **1 CEO** - The CEO owns and manages the company and is responsible for coordinating day-to-day activities. Other duties include: **001**
 - Issue RFID access
 - Managing financial data
 - hiring and termination of employees

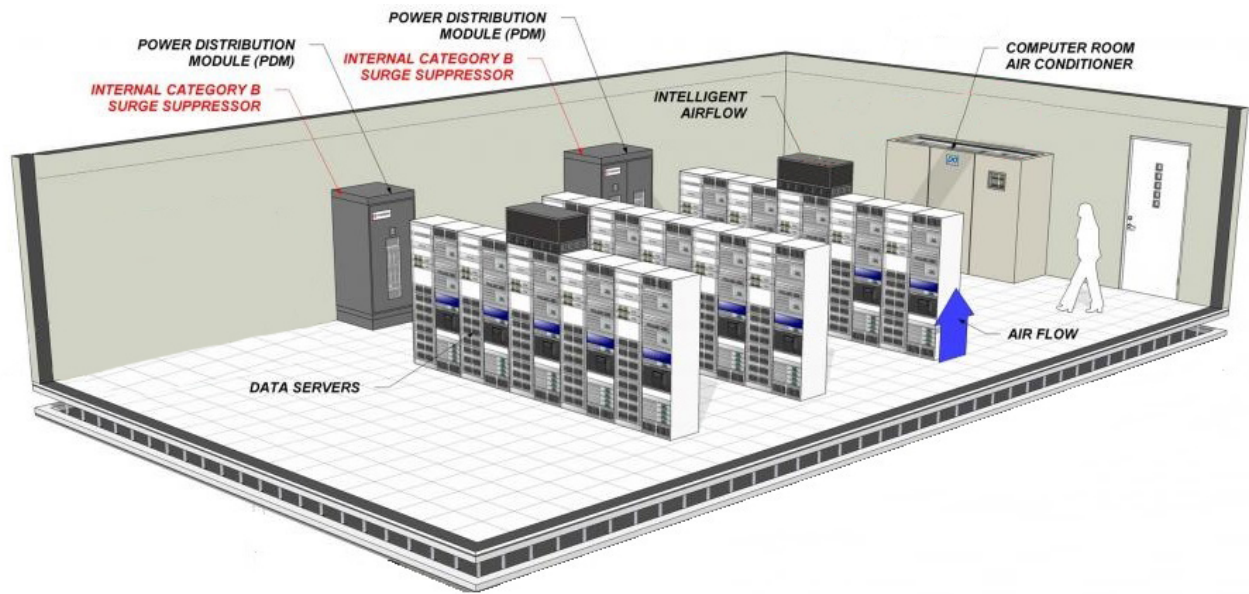
- **2 Engineers** - There are 2 engineers who provide 24/7 support to customers through 12-hours shifts. **002**

Engineers have full access to the user account information. Some of their other duties include:

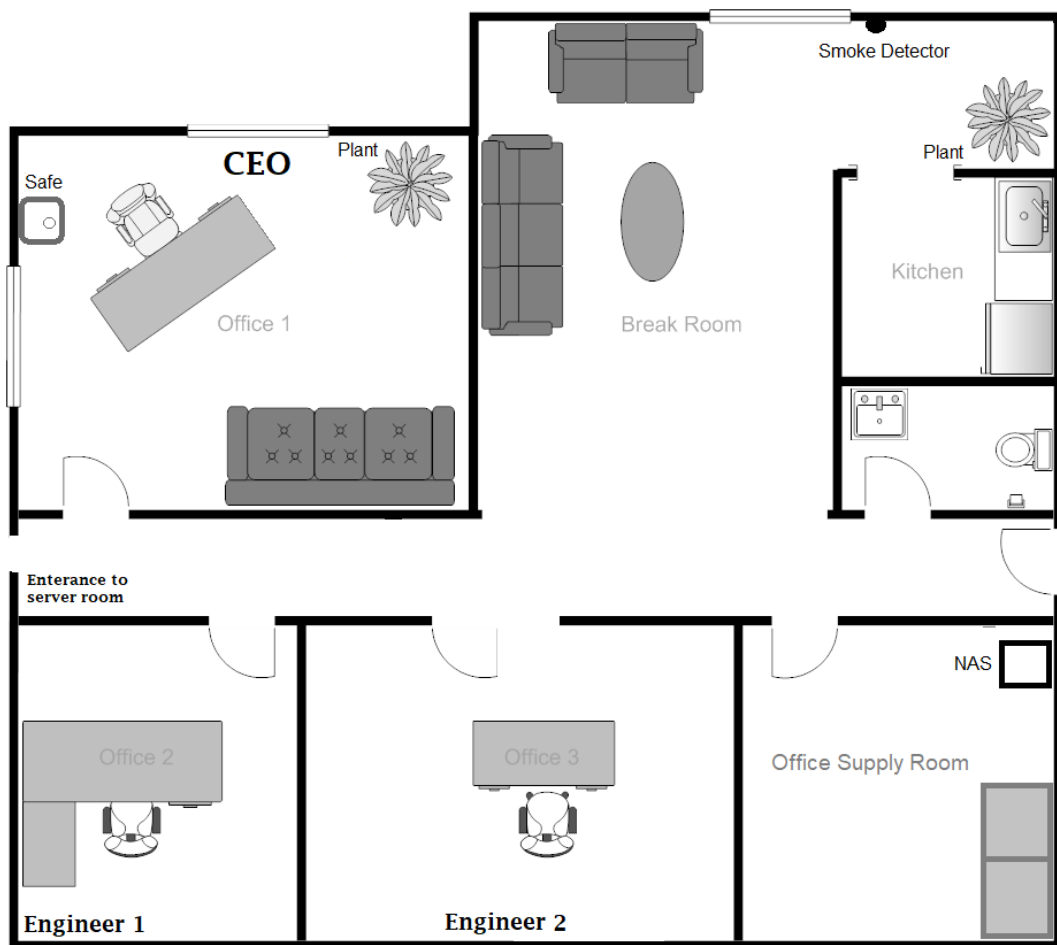
- Register new users
- Activate or deactivate user accounts
- Delete use accounts and data
- Backup
- System maintenance and upgrades
- Password reset

Engineers are also responsible for ensuring all hardware components work properly, manage electrical systems within the data centre, wiring, cooling systems etc.

Server Room



ETHERSPACE Office



Services

ETHERSPACE offers the following services – All Prices are in NZ\$:

Plan	Number of active users	Can Accommodate
Basic	45	50
Advanced	50	60
Premium	80	100


Basic

8 GB Ram
1 TB HDD Storage

- ✓ 1 IPv4-address, 10 IPv6 addresses
- ✓ TUN/TAP available

☐ compare

[Product Details >>](#)




Advanced

12 GB Ram
2 TB HDD Storage

- ✓ 1 IPv4 address, 1 IPv6 /112 subnet
- ✓ TUN/TAP available

☐ compare

[Product Details >>](#)




Premium

16 GB Ram
4 TB SSD Storage

- ✓ 1 IPv4 address, 1 IPv6 /112 subnet
- ✓ TUN/TAP available

☐ compare

[Product Details >>](#)



- All purchases of data centre services are done online through their purchase system. Services are activated once the payments have been successfully processed and validated. Payments are done using an external system (i.e. Google Pay). No credit card information is revealed to EtherSpace employees nor saved locally.
- All services are associated with the customer's number and registered email. **018**
- Data centre outsources its web hosting to a specialised web site and domain management company. They guarantee 99.99 percent uptime. **045**

- The transactional data including the customer information such as customer number, the types of the services purchased, full name, address, phone number and email of the customer are saved every Friday at 11.30 PM on the Network Attached Storage (**NAS**) drive located in the office supply room in .csv format to be easily compatibility with other applications (e.g., Excel). **005 and 019 and 020**
- All employees have an RFID key to access their own office, office supply room and the server room. Engineers do not have access to each other's rooms or the CEO's room. 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. **006**
- 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. **007**
- Each provided RFID key has a unique identifier. The access control system logs each access and saves the information on the CEO's desktop PC. The RFID access software was purchased from <https://gaorfid.com/access-control-software-overview/> for 5000 NZ\$. **022 and 027**
- Account information are emailed to the customer after initial installation and setup (see next page) **008 and 030 and 036**
- Engineers are advised to avoid using their own laptop/device to perform daily tasks. Each engineer is assigned a dedicated Desktop PC. **009 and 049**
- All dedicated PCs used by staff are running latest version of Ubuntu Desktop which is set to update automatically. Staff have full access on the desktop PCs. **010 and 028, 038**
- All internal devices (Desktop PCs, Network Attached Storage) are located within an internal subnet, isolated by a firewall. **029 and 011 and 045 and 044**
- Each staff has own desk, chair, file cabinet and basic stationery. **IGNORE**
- Each server can support up to 20 virtual servers. Servers are managed using a hypervisor which runs on a Debian 11 Linux distribution. All servers are located in the DMZ. There is only one DMZ and all references to the word refer to the same logical subnet. **031 and 032 and 040 and 041**
- Once the VPS services are setup and assigned, customers have full virtual control over the system. This includes creation of user accounts -within the Virtual machine of the VPS assigned to the customer-, installation of software, drivers etc). **012**
- Customers are also granted access to a management interface (web-based at <http://management.EtherSpace.co.nz>) by which they can modify major aspects of their VPS service (e.g. reset the VPS, change operating system (i.e. rebuild), shut down, reboot etc.) (see Figure 1) The server is referred to as **WebM** by staff) **012 and 033**
- Management interface credentials are emailed to the client's registered email (See sample registration email) **007**
- VPS management interface allows customers to reset their VPS to their initial state (. Resetting the VPS systems to initial state takes 5 minutes. Hypervisor then allocates the customer's registered service's processor and RAM and randomly allocates a disk space on an available server to the newly created VPS. All customer data and operating system configuration are deleted in the process. Customers can also use the management interface to cancel their service immediately. They'll be presented with a confirmation link (Figure 1). User account and data are immediately deleted. **013 and 014 and 023**
- The server hosting the management interface is located in the DMZ and managed by the engineers.
- Customers login into their VPS system (1**.209.50.12) using SSH service using root account.

- Customers may phone in or email admin@EtherSpace.co.nz with their service information (Customer number, service information, registered email address and by verifying their address) to reset their **VPS management system passwords**. Engineers are not able to reset the root account password for the operating system instance running on the VPS. **015**
- All ports to and from the DMZ are open for customers (i.e. clients). This allows the clients to connect to their VPS servers using any service and port they wish and also connect to external resources from their VPS server on any port and service. **041**
- CEO keeps employment documents in a safe in his office. He can only access the safe. Other employees cannot access CEO's office if locked. **016 and 021**

Hardware and Equipment

Equipment	Description	Price Per Unit
Servers	Quantity: 24	15,000
Web servers (WebM)	Quantity: 1	
24 Port Switches	Quantity: 11	3000
Routers	Quantity: 3	5000
Data link	Description: 10 Gbps	
Air conditioning systems	Quantity: 1 unit	2500
Smoke detectors	Quantity: 4 units	15
Power Distribution Module	Quantity: 2 units	6000

Software	Price per unit
Firewall	Free
Hypervisor	10,000
Debian 11.0	Free
Customer management software	In-house
OpenOffice	Free

Miscellaneous information

- Data centre has a primary link of 10gbps. The data is routed through New Zealand to United States via Southern Cross undersea cable.
- The data centre does not provide wireless access to its employees for security reasons. **017**
- There are off the shelf battery powered smoke detectors installed (2 in the ETHERSPACE main office and 2 in the server room)
- The data centre enforces strong password policy for engineers. Engineers are therefore expected to use strong passwords for devices. **017**
- All office-related maintenance (e.g. plumbing, cleaning) are managed by external contractors. Temporary access is provided when needed. **01**
- EtherSpace does not allow counter sales of any of their service. All sales are done via their web site. **018**
- EtherSpace does not monitor the customer's data or software on their VPS. **019**
- The employees trust each other and minimum oversight is done. No background check is performed during the job application process.

- Transactional data: all Information about the types of the services the customers have purchased (including customer information (Customer Number, address, email, phone, etc.), service information (see below), the date of the purchase, amount paid...).
- Customer data: Customer data represent information the customer keeps on their virtual machine (example: a photo a customer may upload into the purchased VPS)
- Service information: information displayed on the web site about a service: Basic, Advanced, Premium and sub information (amount of ram, storage etc.)
- The words "Clients" and "customers" are used interchangeably.

Sample Registration Email:

Dear valued customer,
Customer Number: 73667292

Your new VPS has just been provisioned:

Service 1:

Image: Debian 32Bit
RAM / storage: 8GB/1 TB
IP addresses: 1**.209.50.12
User: root
Password: 7HTK9N

Service 2:

Image: Debian 32Bit
RAM / storage: 12GB/2 TB
IP addresses: 1**.209.50.13
User: root
Password: 3HTK7N

VPS management system information:

User: 73667292
Password: EtherSpace65

VPS management system IP address: 1**,209.50.1

It will take approximately 5 minutes from now, until the server is reachable. You can then login to the server using SSH protocol (e.g. "ssh 1**.209.50.12 -l root").

For security reasons we recommend you to change the password for the user "root" right after you logged in for the first time and keep it in a secured place!

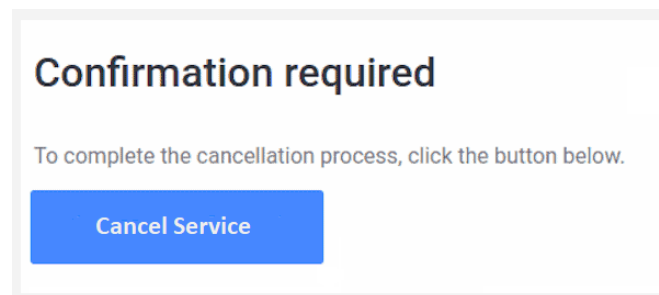
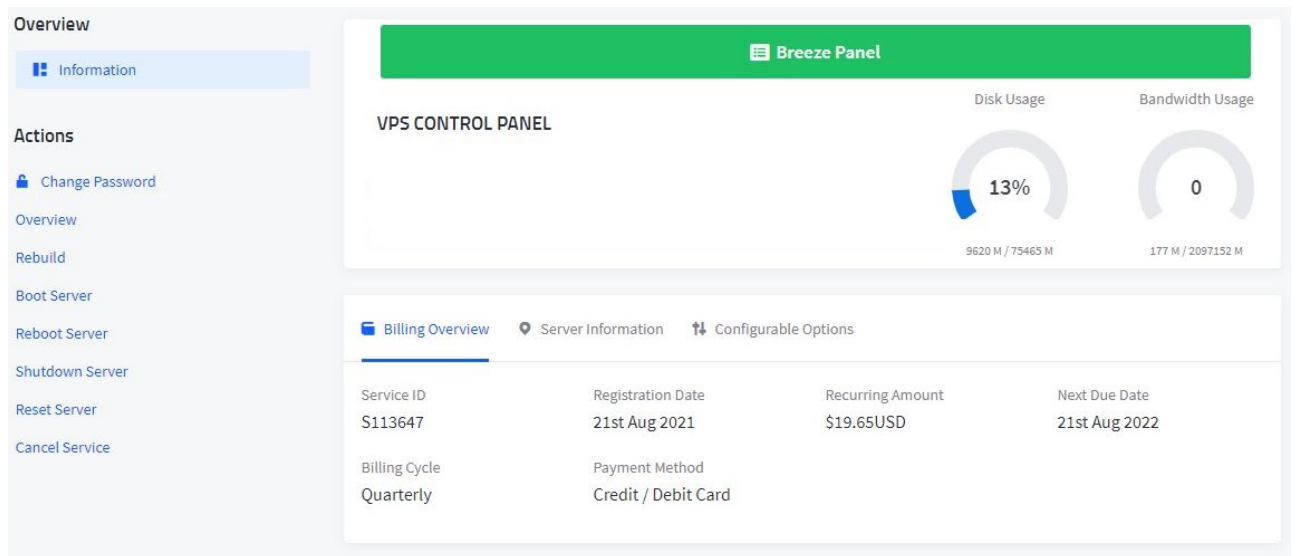


Figure 1- VPS management interface and cancellation confirmation

Tasks:

Provide the appropriate risk management documentation for the data centre.

Your final report must have the following sections (minimum requirements).

Total: **38 Marks**

- a. Rating and classification definitions:

3 Marks

- b. Asset identification and classification (i.e. Information asset classification worksheet)

10 Marks

- c. Risk assessment worksheet (i.e. Risk calculation), including threat and vulnerability assessment (e.g. identification and description of each threat and vulnerability for each asset, impact and likelihood of each risk)

10 Marks

- d. Current and proposed control strategy for each vulnerability/threat/risk, residual risk and the escalation path. **Please refer to “Points to consider” section and grading criteria for additional information.**

10 Marks

- e. Writing, presentation of the report and referencing

5 Marks

Cost Benefit Analysis is NOT required. (Qualitative analysis is recommended and sufficient)

Points to consider:

- Do NOT make any assumptions! If you “HAVE TO” make any assumptions, then all assumptions must be explicitly mentioned at the beginning of the document. Qualitative and quantitative measurements should be defined early in the document. E.g.:
 - What 7/10 or “likely” means
 - What private, public, confidential etc. means
 - What low, medium or high means
 - Any other scaling, rating or classification you may use
- During identification and prioritisation of threats, provide a brief description of the threat and give an example; clearly state how each threat can be a risk to an asset. Description of threats can be referenced from reliable sources but in no shape or format copied or plagiarised. (Books, journals, conference publications, ISO/NIST documents, Technical reports (e.g. SANS institute documents)).

- While determining the likelihood of threats, consider referencing reliable sources and reference them accordingly. Reliable sources include Books, journals, conference publications, Technical reports e.g. SANS institute reports.
- Avoid proposing unnecessary and unjustifiable controls for the identified risks **at all cost**. Unnecessary controls result in waste of resources (e.g. cost of purchase, cost of installation, cost of maintenance, other resources such as power, space, staff allocation etc.). Proposing controls without justifications will result in reduced points.
- Use standard templates for any of the above phases. You may research and find a number of standard templates or use the ones from the book. **An incomplete example template has been provided**. You may restructure the tables, labels and everything else in the given template to suit your content or style. You must add additional information to achieve the highest grade.
- You may use any available methodologies. These include but not limited to:
 - OCTAVE
https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf
 - NIST <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- Structure, flow, readability, depth of analysis, attention to detail, presentation of the document and proper referencing are important.

Grading Criteria:

- **Completeness** – Did you complete all the tasks and how comprehensively? Did you provide explanation where necessary? examples:
 - Did you list all the assets and identified their classification? Are those classification sound and justifiable?
 - Did you value the assets based on their impact to profitability and public image?
 - Did you list all the threats and associated vulnerabilities for each asset? Are those vulnerabilities and threats based on facts and justifiable?
 - Did you list the current controls in place for each threat/vulnerability?
 - Did you propose additional controls to mitigate or minimise the risk?
- **Accuracy** - How well did you complete the tasks? examples:
 - Did you correctly assign severity and likelihood to each threat and vulnerability for each asset? Is the assigned severity and likelihood justifiable? Can you provide a reference for the severity and likelihood values given?
 - Did you propose the correct controls for each threat? Does the control minimise the likelihood or the impact of a threat? Are they properly justified for the identified risk?
- **Presentation** - Did you use the right terminology? Are your tables properly structured? Is the line/paragraph spacing consistent across the report? Please check for readability. A well-structured and well-written report is expected.

Letter Grades

A-range:

Complete, accurate, and well presented. Shows good knowledge and good understanding of methods. **Well-argued. Where required, contains good original input from the student. Must present exceptional report according to the criteria for each task.**

B-range:

Mostly complete, mostly accurate, and well presented. Shows a good knowledge and fairly good understanding of the methods but either fails to complete some parts of the tasks or is unclear or is poorly argued.

C-range:

Satisfactory performance although some errors in accuracy and/or problems with presentation. Shows only some basic knowledge of the material or fails to understand some important parts of it, or does not provide solutions to a significant portion of the tasks.

D-range:

Poor performance overall, some evidence of learning but very problematic in all aspects mentioned above.

E-range:

Well below the required standard.