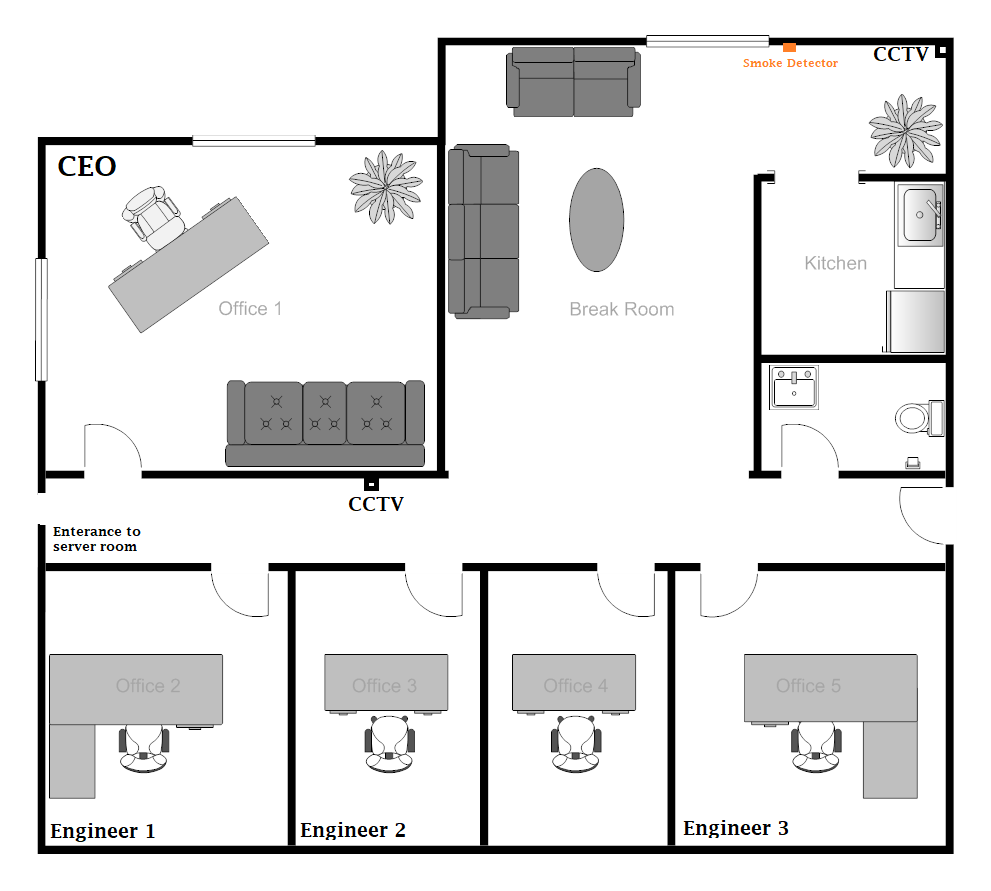
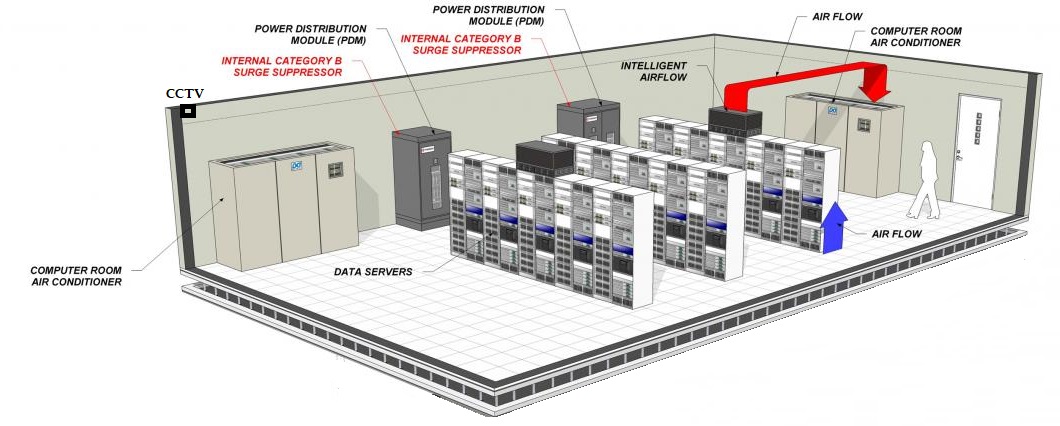
**Assignment 1**

**Due Date: 16/8/2020**

**HostNZ** is a small sized datacentre located in Auckland, New Zealand. HostNZ provides Virtual shared and dedicated Private Servers (VPS) to consumers in New Zealand. The datacentre is located at the heart of Auckland Central Business District (CBD). The company relocated to the new datacentre 2 years ago. Businesses located in Auckland contribute to a large portion of HostNZ’s customers at the moment.



**Organisational Structure**

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

* 1 CEO
* 3 Engineers

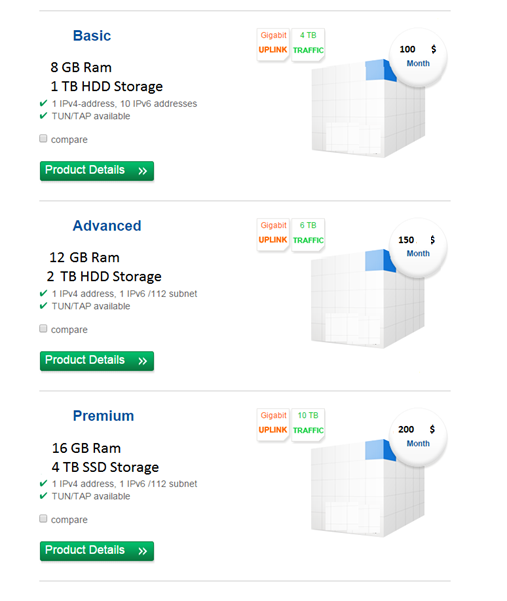
**Roles**

* The CEO owns and manages the company and is responsible for coordinating day-to-day activities. Other duties include:
  + Issue access cards
  + Managing financial data
  + hiring and termination of employees
* There are 3 engineers who provide 24/7 support to customers through 8-hours shifts.
* Engineers have full access to the user account information. The list of their privileges include:
  + Register New users
  + Activate or deactivate user account
  + Delete use accounts and data
  + Data Recovery
  + System maintenance and upgrades
  + Password reset
* Engineers are also responsible for ensuring all hardware components work properly, manage electrical systems within the datacentre, wiring, cooling systems etc.

**Services**

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

|  |  |  |
| --- | --- | --- |
| **Plan** | **Number of active users** | **Can Accommodate** |
| Basic | 40 | 50 |
| Advanced | 50 | 50 |
| Premium | 80 | 100 |



* All purchases of datacentre 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. Paypal). No credit card information is revealed to HostNZ employees nor saved locally.
* All services are associated with the customer’s number and registered email.
* The transactional data including the types of the services purchased, full name, address, phone number and email of the customer are saved locally on a local system in an Oracle Database which is backed up using a cold back up technique every Friday at 11.50 PM. The backup files are saved on an external drive kept at a locked drawer at the office. Engineers are each issued a copy of the key.
* Account information are emailed to the customer after initial installation and setup (see next page)
* All dedicated PCs used by staff are running Debian 7 with default installation services and features.
* Each server can support up to 20 virtual servers. Servers are managed using a hypervisor which runs on a Debian 7 Linux distribution.
* Once the VPS services are setup and assigned, customers have full virtual control over the system. This includes creation of user accounts (within the VPS system), installation of software, drivers etc).
* Snort intrusion detection system monitors internal and customer network for signatures of attacks.
* Customers login into a unique system (1\*\*,209.50.1) using SSH service and enter their VPS management system details to reset their VPS to their initial state. All customer data is deleted in the process.
* Customers may phone in or email [admin@hostnz.co..nz](mailto:admin@hostnz.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 may then reset the virtual servers to their initial state (clean installation) with default password (HostNZ).
* Resetting the VPS systems to initial state takes 15 minutes.
* Customers can download the cancellation form and email it to admin@hostnz.co.nz with their service information (Customer Number, service information, registered email address and by verifying their address) to cancel their service. User account and data are deleted 72 hours after submission of the application.
* Datacentre manages its own web hosting. The web server is located in the DMZ and strict firewall policies are enforced. The server is also installed on a hardened bastion host with strict security measures implemented (e.g. removed unnecessary packages, services and closing of ports. Default accounts were removed.). A disk-level backup copy of the webserver is created every Friday and saved on an external drive and kept with the customer data in the locked drawer.
* The locked drawer is located in the CEO’s office but is accessible to all employees.
* CEO keeps employment documents and transactional data in a safe in his office. He can only access the safe.

**Hardware and Equipment**

|  |  |  |
| --- | --- | --- |
| Equipment | Description | Price Per Unit |
| Server | Quantity: 24 | 15,000 |
| Web/application server | Quantity: 1 |  |
| 24 Port Switches | Quantity: 11 | 3000 |
| Routers | Quantity: 3 | 5000 |
| Primary data cabling | Description: 10gbps primary link |  |
| Secondary data cabling | Description: Fail over 1gbps link |  |
| Air conditioning systems | Quantity: 6 units | 2500 |
| CCTV | Quantity: 3 units | 400 |
| Smoke detectors | Quantity: 4 units | 15 |
| Fire extinguishers | Quantity: 10 units | 220 |
| Power Distribution Module | Quantity: 2 units | 6000 |

|  |  |
| --- | --- |
| **Software** | **Price per unit** |
| Firewall | Free |
| Hypervisor | 10,000 |
| Debian 7.0 | Free |
| CCTV Security Surveillance Software | Included with hardware |
| Customer management software | In-house |
| OpenOffice | Free |

**Miscellaneous information**

* Datacentre has two primary links, a 10gbps primary link and one 1gbps link in case of failure of primary link. Two primary links are registered with two different companies (i.e. Vodafone, Orcon) and routed through New Zealand to United States via Southern Cross undersea cable.
* The datacentre does not provide wireless access to its employees for security reasons.
* Engineers are advised to avoid using their own laptop/device to perform daily tasks. Each engineer is assigned a dedicated station at the office.
* Physical access for staff is provided by the CEO through access cards. Cards expire every 18 months.
* Access to the main office and server room is done via the cards and secured doors. All employees have full physical access to all sections of the datacentre.
* There are off the shelf battery powered smoke detectors installed (2 in the office and 2 in the server rooms)
* CCTV cameras record activities and keep the video for 3 days. The data is then rewritten.
* The datacentre does not enforce strong password policies for engineers. Engineers are however expected to use strong passwords for devices.
* 10 Class E fire extinguishers are spread across the datacentre floor in case of fire.
* All office-related maintenance (e.g. plumbing, cleaning) are managed by external contractors. Temporary access is provided when needed.
* Each staff has own desk, chair, file cabinet and basic stationery.
* HostNZ does not allow counter sales of any of their service.  All sales are done via their web site.
* Customers own any software installed and are responsible for software licenses.
* Customers own any data stored and are responsible for the content.
* 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 ..), 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 website about a service: Basic, Advanced, Premium and sub information (amount of ram, storage etc)
* Transactional logs=transactional data!

**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\*\*.209.50.92  
User:            root  
Password:        1HTK9NZ

**Service 2:**  
Image:           Debian 32Bit  
RAM / storage:   12GB/2 TB  
IP addresses:    1\*\*.209.50.93  
User:            root  
Password:        3HTK7NZ

VPS management system information:

User:            73667292  
Password:        HostNZ65

VPS management system IP address: 1\*\*,209.50.1

It will take approximately 15 minutes from now, until the server is reachable.  
You can then login to the server using SSH protocol (e.g. “ssh 1\*\*.209.50.92 -l root”).  
  
For security reasons we ask you to change the password for the user "root" right after you logged in for the first time!

**Tasks:**

Provide the appropriate risk management documentation for the data centre.

Your final report must have the following sections (minimum requirements). Total **100 Marks**

* 1. Introduction and overview 2 Marks
  2. Roles definition and responsibilities 3 Marks
  3. Rating and classification definitions 5 Marks
  4. Asset Identification (Information asset classification worksheet,

Weighted criteria analysis worksheet) 15 Marks

* 1. Asset categorization and classification 10 Marks
  2. Identified threats, description, their likelihood and severity 20 Marks
  3. Identified vulnerabilities, description, likelihood and severity (Ranked

vulnerability risk worksheet) 20 Marks

* 1. Current and proposed control strategy for each vulnerability/threat 20 Marks

**Writing and presentation** 5 Mark s

Cost Benefit Analysis is **NOT** required.

**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
* 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 much fewer marks than one you have written in your own words.

**Points to consider:**

* Do not make assumptions unless completely necessary. Any 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 or classification you may use
* During identification and prioritization 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 plagiarized.
* While determining the likelihood of threats, consider referencing reliable sources and reference them accordingly.
* 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. **Use of the provided template is recommended.** You may restructure the tables to suit your content or style.
* There are no word limits for the final document. Structure, flow, readability, depth of analysis, attention to details, presentation of the document and proper referencing are very important.

**The criteria for grading are:**

* 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?
  + Did you valuate the assets based on their impact to profitability and public image?
  + Did you list all the threats and associated vulnerabilities for each asset?
  + 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?
  + Did you propose the correct controls for each threat?
* Presentation - Did you use the right terminology? Please check for readability, we mark a lot of these and generally we look more favourably on well-structured and well-written ones.

**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.

**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.