**22334VIC – Certificate IV in Cyber Security**

**VU21992 – Develop a cyber security industry project**

**Assessment Task 2 –** **Project Implementation**

|  |  |
| --- | --- |
| **Student Name** | **GIUSEPPE RACITI** |
| **Student ID** | **S3113490** |

**Instructions**

This assessment must be completed in teams as approved by the Instructor.

This assessment is self-paced but recommended to be completed as detailed in the Unit Guide.

Plagiarism is not tolerated. You must acknowledge sources of information you use in your writing. You must reference whenever you quote, paraphrase or summarise someone else’s ideas (see [https://www.vu.edu.au/library/get-help/referencing/referencing-guides](about:blank) for further information).

Create a single document containing your responses to all of the tasks listed below. Submit your work as a single PDF file to the VU21992 Assessment Task 2 Dropbox in VU Collaborate.

You must include the following information on all items submitted for assessment:

* The names of your team members
* The Student IDs of your team members
* The date submitted
* 22334VIC – Certificate IV in Cyber Security
* VU21992 – Develop a Cyber Security industry project
* Assessment Task 2 – Project Implementation

**Overview**

You must manage and execute the implementation of cyber protections for the OZCazual network in line with the plans you developed in Assessment 1 with your team. It is expected that you will implement the items which were assigned to you in assessment 1, unless otherwise agreed on with your team.

You must produce appropriate configuration management records for ALL physical and virtualised equipment in the revised network, including:

* Virtualised hardware manifests for virtualised equipment
* Configuration files/scripts and build documentation for any additional equipment/software
* It is not necessary to record serial number etc for components of equipment – a simple of constituent items and their descriptions such as capacity, speed etc is adequate.

**Task 2.1 Reconfigure Network Infrastructure**

You must reconfigure the existing network infrastructure to better protect the OZCazual ICT operations. This may include any or all of:

* Redesigning the network topology including topology diagrams with per-port addressing
* Installation/removal of new/existing network equipment
* Reconfiguration of existing equipment
* Introduction of new security procedures/practices/facilities such as 2FA, secure connection etc.

This reconfiguration should be arranged so as to minimise interruption to business operations.

You should also execute your test plans for each piece of routing/switching/firewalling infrastructure. Remember to produce appropriate configuration management records for your new network infrastructure.

**Task 2.2 Install/Upgrade Application Systems**

You must install or upgrade all current OZCazual application systems to the revised network infrastructure. This may include any or all of:

* Upgrading existing systems in the new infrastructure
* Installing new systems to replace the existing application systems.
* Installing additional systems to further enhance the security of the infrastructure.

This migration should be arranged so as to minimise interruption to business operations, unless otherwise stated in the project planning stage for assessment 1

You should also execute your unit test plans for each application system. Remember to produce appropriate configuration management records for the application systems.

**Task 2.3 Install & Configure Security Systems**

You must implement Cyber Security tools such as:

* Server Traffic Monitors
* Log analysis systems
* Anti-Virus/Malware systems
* Internal Firewalls
* Suitable resources for remediation of compromised systems in the event of a cyber incident.

You should also execute unit test plans for all components of your Security systems. Remember to produce appropriate configuration management records for the Security systems.

Install & configure Kali Linux on the AWS network, this will be used for penetration testing in Task 3.3

**Task 2.4 Develop Formal End-to-End Test Plans**

You must develop end-to-end test plans for each supported application system, obtaining agreement from line-of-business managers that the test plans are adequate. These plans must include explicit statements of the processes and procedures to be followed to test each application system.

**Task 2.5 Execute End-to-End Testing & Remedy Deficiencies**

You must execute end-to-end testing as developed in task 2.4, obtaining sign-off from line-of-business managers. If modifications to your plans are required ensure that you update the appropriate configuration management records.

**Task 2.6 Finalise New System Operational/Support Processes & Documentation**

You must prepare revised Operational & Support processes and documentation to allow the continued management of the revised infrastructure. This should include as a minimum:

* Start-up & shutdown procedures
* Backup & recovery from backup procedures
* Regular maintenance activities with a schedule of execution.

In addition, you must produce a final report for the system designed documenting:

* Which elements were delivered as designed
* Which components were not delivered
* Which components were modified from the original design and the nature of the modifications