| **PROJECT SCOPE** | | | | | |
| --- | --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | **15th of June, 2023** |
|  |  |  |  | |  |
| Project Manager: | **Giuseppe Raciti** |  | Project Sponsor: | **OzCazual** | |
|  |  |  |  |  | |
| Project Started: | **12th of June, 2023** |  | Projected Finish date: | **14th of July, 2023** | |

| **Project Scope Description** | | | | | |
| --- | --- | --- | --- | --- | --- |
| The AWS CyberShift Initiative project will secure OzCazual's cloud infrastructure and enable a safe and secure migration from their existing local server to Amazon AWS.  The primary goal is to address the sudden 200% increase in online sales and staff, create a scalable infrastructure that can meet future business demands, and ensure the confidentiality, integrity, and availability of the systems and customer data.  The project will Implementing various security controls, and upgrade the systems and tools currently used at OzCazual | | | | | |
| **In Scope** | | | | | |
| The following are **in scope**:   * Redesign of the current network infrastructure and topology * Installation and configuration of security and monitoring software of:   + Windows Server 2019, and   + Amazon Linux 2 web server * External scans and attack simulations using various tools * Red team / blue team exercises to test system vulnerabilities * Handover of technical documentation upon project completion   The following points are **not in scope**:   * Physical security aspects, such as access control to physical server rooms of the cloud service provider * Procurement management - including the purchasing of hardware or software, is also excluded * Ongoing maintenance and support: Once the project is completed and the cloud infrastructure is secured, the responsibility for ongoing maintenance and support of the infrastructure will not be part of this project. | | | | | |
|  | | | | | |
| **Project Deliverables** | | | | | |
| 1. **Secure the cloud infrastructure**  * Install and configure secure Windows 2022 AD Server:   + Firewall configured - **pfSense** or Windows Defender   + IPS/IDS - **Snort**   + Anti-virus/malware protection - **Sophos**   + Log monitoring and analysis - **Splunk**   + Real-time monitoring - **Wireshark** * Install and configure secure Linux Web Server:   + Firewall - **Sophos**   + IPS/IDS - **Snort**   + Anti-virus/malware protection - **Sophos Intercept X**   + Log monitoring and analysis - **Splunk**   + Real-time monitoring - **Wireshark**  1. **Perform external scans/vulnerability assessments:**  * Using a tool called Infection Monkey, conduct automated scans for possible vulnerabilities * Scans conducted on Windows Server 2019 to identify vulnerabilities * Scans conducted on Amazon Linux 2 web server to identify vulnerabilities * Vulnerability report generated with identified issues and recommendations for mitigation  1. **Red / blue team exercises:**  * Red team exercise conducted on Windows Server 2019 and Linux web server * Vulnerabilities and weaknesses identified and documented * Blue team response and remediation actions implemented to address identified vulnerabilities  1. **Handover of technical documentation:**  * Configuration documentation for secure cloud infrastructure * Security policies and procedures documented * Incident response plan and procedures developed * Security guidelines and best practices compiled * Documentation reviewed, approved, and signed off | | | | | |

| **Work Breakdown Structure (WBS)** | | | | | |
| --- | --- | --- | --- | --- | --- |
| The WBS used in this project is organized based on the Agile approach, also using a Gantt chart to visualize the timeline of the project's milestones and events.  Using a SCRUM system, the project is broken down into 3 Sprints consisting of the Planning, Implementation and testing, and penetration and documentation phases, which will also include a final report with results and mitigation strategies.  The estimated budget for the project is predicted to be around $35,000, not including the cost of equipment procurement and software licenses.  Below, is a detailed outline of the 3 sprints   | **SPRINT ONE** | | --- | | Task 1.1 - Project Requirements Definition  Task 1.2 - Define Project Scope  Task 1.3 - Assemble Project Team & Allocate Responsibilities  Task 1.4 - Develop Work Breakdown Structure & Allocate Resources  Task 1.5 - Prepare Scope, Quality, Budget, Schedule, Comms Management Plans  Task 1.6 - Finalize Project Plan and Obtain Approval | | **SPRINT TWO** | | Task 2.1 - ReConfigure Network Infrastructure  Task 2.2 - Install/Upgrade Application Systems  Task 2.3 - Install & Configure Security Systems  Task 2.4 - Develop Formal End-to-End Test Plans  Task 2.5 - Execute End-to-End Testing & Remedy Deficiencies  Task 2.6 - Finalize New System Operational/Support Processes & Documentation | | **SPRINT THREE** | | Task 3.1 - Prepare Handover Documentation  Task 3.2 - Review Project Team Performance  Task 3.3 - Execute Red-Blue Testing  Task 3.4 - Obtain Sign-Off & Close Project |   The WBS provided is only a high-level breakdown of the activities and tasks involved in the Agile project scope management plan, aligned with the SCRUM system of 3 sprints. Each sprint consists of other specific tasks and subtasks which are Gantt charts to provide a visualization of the progress of the project. This can be accessed through the WBS provided in the project | | | | | |

| **Scope Change Management** | | | | | |
| --- | --- | --- | --- | --- | --- |
| During the course of the project lifecycle, to effectively manage scope changes, any modifications or changes that are required to the original scope will require an official ‘Change Request’ through the Change Management plan.  The Change Management Plan Process below, is a brief explanation of what is required when any stakeholder requires changes to the original scope.   * Submit a formal change request, detailing the change and supporting documents * Project Manager and team assess the impact to the project objectives, scope, schedule, budget and risks. * Change request is reviewed by an appointed committee, ensuring the change is aligned with the project goals * The Committee will approve or deny the request, based on an evaluation and review * The approved change will be integrated and reflected in the project plan, schedule, budget and risks as necessary * The impact of any approved changes, are documented in the change log * The Project Manager ensure that the is no scope creep from any of the approved changes   By following the Change Management Plan process, this helps to mitigate scope creep during the lifecycle of the project, and avoid delays or unauthorized changes that would otherwise cause changes to the project scope, budget, schedule or risks | | | | | |

| **Approvals:** |
| --- |
| |  |  |  | | --- | --- | --- | | Project Manager Signature |  | Sponsor Or Originator Signature | |  |  |  | | Project Manager Name |  | Sponsor Or Originator Name | |  |  |  | | Date |  | Date | |