| **PROJECT CHARTER** | | | | | |
| --- | --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | **13th of June, 2023** |
|  |  |  |  | |  |
| Project Manager: | **Giuseppe Raciti** |  | Project Sponsor: | **OzCazual** | |
|  |  |  |  |  | |
| Project Started: | **12th of June, 2023** |  | Projected Finish date: | **14th of July, 2023** | |
|  |  |  |  |  | |
| **High-Level Project Description** | | | | | |
| The objective of the project is to securely migrate OzCazual's existing infrastructure, which includes a Windows 2022 and Linux Web Server, to the Amazon Web Services (AWS) cloud platform, and enable safe and secure migration from their existing local server.  The aim of the project is to address the sudden 200% increase in sales and new staff at OzCazual, and provide infrastructure scalability to meet future business demands, while ensuring confidentiality, integrity, and availability of the systems and customer data.  The migration will be performed by SecureNET under the project name ‘AWS CyberShift Initiative’, and is a reputable cyber security company that will ensure the migration is performed safely, while maintaining the integrity of the cloud environment. The cyber team will implement robust security measures, including firewalls, intrusion detection systems, antivirus/malware protection, log monitoring and analysis systems, and real-time monitoring tools.  The project will also include an approved external vulnerability scan, which involves red team/blue team exercises, to test the AWS environment against various types of attack methods.  The project will follow the SANS framework, a widely recognised and comprehensive cybersecurity framework, that will guide the implementation of security controls required to secure both the local and cloud infrastructures.  Upon project completion, all technical documentation will be signed off and handed over to OzCazual | | | | | |
| **Project Background Information:** | | | | | |
| OzCazual, an e-commerce company, has experienced a sudden 200% increase in online sales, resulting in the need to scale their local server infrastructure. To meet the increased demand and ensure the security of their systems and customer data, OzCazual has decided to migrate their services to the Amazon AWS cloud infrastructure. However, before the migration can proceed, it is crucial to secure the cloud environment to protect against potential cyber threats.  OzCazual has hired our Cyber Security firm, SecureNET, to handle the task of securing their newly deployed cloud infrastructure. The primary objective of this project is to implement robust security measures in the cloud environment, allowing for a safe and secure migration from the existing local server. By ensuring the confidentiality, integrity, and availability of the systems and customer data, OzCazual aims to meet the increasing business demands effectively. | | | | | |
|  | | | | | |
|  | | | | | |
| **Project Success Criteria:** | | | | | |
| **Secure the cloud infrastructure:**   * Ensure that the AWS cloud infrastructure is secure, including the local servers: Windows Server 2022, Linux Web server * Implement robust security systems, such as firewalls, IDS/IPS, anti-virus/malware protection, log monitoring and analysis systems, and real-time monitoring tools. * Additionally, enforce the use of Two-Factor Authentication (2FA) for all user accounts to enhance authentication security   **Configuration:**   * Configure firewalls, IPS/IDS, Anti-virus/malware, and Two-Factor Authentication * Ensure all systems have been tested and working correctly.   **Perform vulnerability testing:**   * Perform external pen-testing exercises on both the AD server and Web Server, where real-world type attacks will be used to simulate attack scenarios to expose vulnerabilities and assess the security posture of the implemented security measures, including the Two-Factor Authentication (2FA) effectiveness. * The exercise will test detection and defense against various attack methods.   **Stakeholder Satisfaction:**   * Meet with the OzCazual Management, Server Administrators, and end-users, effectively respond to any concerns that might have been raised. * Deliver a secure and reliable cloud infrastructure that meets the needs and expectations of the sponsor. * Ensure the project remains within the budget and timeline as detailed in the project scope. | | | | | |
| **Key Deliverables:** | | | | | |
| * Produce a comprehensive report of the existing local infrastructure. * Produce documentation that outlines the cloud infrastructure security * Configure and secure the cloud environment * Produce documentation that details the implemented security controls and measures. * Safely and securely migrate the services from the existing infrastructure, to the cloud system * Test reports detailing red-blue team simulated exercises, testing the security of the cloud environment * Implement Incident Response Plans (runbooks) and monitoring systems * Produce detailed training materials on security awareness | | | | | |
| **Migration Strategy:** | | | | | |
| 1. Assess the current infrastructure and identify the necessary modification and/or enhancements required, then redesign the infrastructure that aligns with cloud best practices, and implementing robust security controls to protect the network from possible security threats 2. Upgrade the current AD Windows 2022 Server and configuration.  * Introduce Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and divide the network into separate segments or VLANs based on security requirements * Install and configure   + **pfSense** - Firewall   + **Sophos** - Anti-virus/malware security   + **Snort** - IPS/IDS   + **Splunk** - Log monitoring and analysis   + **Wireshark** - Real-time monitoring * Perform testing and validation to ensure all software has been configured properly. * Perform ongoing maintenance and updates  1. Upgrade the current Linux Web Server and configuration.  * Design and configure a separate network segment for the DMZ, isolated from the internal network and the internet, to ensure better security between the Linux server and internal infrastructure. * Install and configure   + **Sophos** - Firewall   + **Sophos Intercept X** - Anti-virus/malware security   + **Snort** - IPS/IDS   + **Splunk** - Log monitoring and analysis   + **Wireshark** - Real-time monitoring * Perform testing and validation to ensure all software has been configured properly. * Perform ongoing maintenance and updates  1. Run testing and analysis on the MFA security mechanisms, ensuring authentication is required for user account logins. Implement MFA for all users, especially for users with elevated privileges. 2. Perform thorough testing and validation, to ensure proper functionality and compatibility of all software on both the Linux Web Server and AD Windows 2022 Server. | | | | | |
|  | | | | | |

| **Roles and Responsibilities** |
| --- |
| | Project Owner - Hettige Jayatissa | | | --- | --- | | **Organization / Position** | **OzCazual** | | **Role Responsibilities:** | * Defines the project objectives * Provide project direction and guidance * Manage project stakeholders * Approve project deliverables * Make decisions and resolve issues * Manage project constraints * Ensure project success * Participate in project governance * Act as a liaison between the project team and senior management | | **Project Manager** - Giuseppe Raciti | | | **Organization / Position** | **SecureNET** | | **Role Responsibilities:** | * Overall project coordination and management * Plan, organize, and control project activities * Ensures project deliverables are completed on time and within budget * Risk management and mitigation * Stakeholder Communication and Reporting | | **Cyber Security Specialist** - Shaun Heywood | | | **Organization / Position** | **SecureNET** | | **Role Responsibilities:** | * Conduct assessments of the existing infrastructure * Design and implement security measures for the cloud infrastructure * Configure and manage firewalls, IPS/IDS systems, and antivirus/malware protection * Oversee testing and incident response * Monitor and analyze logs for potential security threats or breaches * Provide guidance on security best practices * Collaborate with the project team to address security vulnerabilities and risks | | **Cloud Architect / Engineer** - Mark Byrne | | | **Organization / Position** | **SecureNET** | | **Role Responsibilities:** | * Designing and configuring the cloud infrastructure on Amazon AWS * Setting up network connectivity with on-site systems * Ensuring scalability and high availability of the cloud environment * Collaborating with the Cyber Security Specialist to implement security measures * Monitoring and optimizing cloud infrastructure performance * Providing technical expertise on cloud architecture and services | | **Server Administrator** - Mauricio Guerra | | | **Organization / Position** | **SecureNET** | | **Role Responsibilities:** | * Collaborating with the project team to ensure a secure transition to AWS * Assisting in the migration of systems and data to the cloud environment * Configuring and managing the Windows Server 2019 Active Directory server * Supporting the setup and configuration of the Amazon Linux 2 web server * Providing technical assistance during the transition phase * Ensuring the smooth operation of the server infrastructure in the cloud environment | |

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