**PROJECT REQUIREMENTS DEFINITIONS**

**GENERAL PROJECT INFORMATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **PROJECT NAME** | | **PROJECT MANAGER** | **PROJECT SPONSOR** |
| **AWS CyberShift Initiative:  "Shifting Cybersecurity to the AWS Horizon"** | | Giuseppe Raciti | **OzCazual** |
| **EMAIL** | **PHONE** | **ORGANIZATIONAL UNIT** | |
| sales@securenet.com.au | (03) 97499 0528 | **SecureNET** | |

|  |  |  |
| --- | --- | --- |
|  | **System Version** | **Document Version** |
| **VERSION** | **1.0** | **1.0** |

**PROJECT OVERVIEW**

|  |
| --- |
| PURPOSE OF PROJECT |
| The objective of this project is to migrate OzCazual's e-commerce website and Active Directory from the local web server running Windows Server 2022 to a cloud environment. Due to a sudden increase in online sales and staffing, the existing infrastructure is unable to meet the demand, necessitating the migration. |
| DESCRIPTION OF PROJECT |
| After completing the planning phase of the AWS CyberShift Initiative, SecureNET will assess the existing network infrastructure, and design a secure network infrastructure on an AWS cloud system, and safely and securely migrate the operations of OzCazual to the newly designed cloud-based network. SecureNET will obtain and configure all the equipment and software |
| PROJECT OBJECTIVES |
| * Design and implement a secure Amazon AWS cloud environment that can accommodate the increase in online sales and staff, which also has the scalability to manage future growth * The primary objective of the project is once the new AWS cloud infrastructure is implemented, SecureNET will do its best to implement robust security measures to protect the cloud system. This includes aspects such as access controls, encryption, authentication, and the authorization mechanisms to safeguard the system from cyber attacks * Implement strong authentication mechanisms, including Two-Factor Authentication (2FA), to enhance the security of user access to the cloud infrastructure * SecureNET will ensure smooth migration which will allow a seamless transition from the local infrastructure to the cloud environment, all while minimizing any downtime or disruption to normal business operations. * Ensure that the cloud infrastructure SecureNET has implemented adheres to the relevant compliance regulations, industry standards and best practices, to maintain the trust of the customers and stakeholders. * Enhance data confidentiality, integrity, and availability * Implement an Incident Response Plan that proactively monitors, detects, and responds to security incidents effectively, to minimize the possible downtime and impact caused to OzCazual |
| EXPECTED DELIVERABLES |
| The project has the following key outcomes:   * 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 |

**PROJECT SCOPE**

|  |
| --- |
| WITHIN SCOPE |
| * Assess the security of the current network infrastructure, and resign the network topology * Design, implement and configure the security of the AWS cloud environment * Configure firewall, intrusion, and detection prevention systems * Develop and implement new security procedures and policies * Develop and execute a formal red-blue team exercise to test new systems * Provide training and awareness of company employees on cloud security best practices |
| OUTSIDE OF SCOPE |
| * The team is limited to securing the data migration and management to the cloud infrastructure. Activities that relate to back up of local network data to the cloud environment, optimization of the stored data, or data governance are not within the project scope. * Physical security measures of the cloud provider’s systems, such as surveillance, access controls, or security procedures. * Upgrades or modifications to the underlying network infrastructure, which enables communication and connectivity within the organization. This includes the switches, routers, firewalls, etc. |

**RESOURCES**

|  |  |
| --- | --- |
| PROJECT TEAM | The project manager is responsible for the overall project coordination, planning and ensuring the project runs as scheduled, delivering on the promised timeline.  **Cyber Security Specialist:** Shaun Heywood  This role is responsible for conducting assessments, designing, and implementing security measures, and overseeing the testing and incident response.  **Cloud Architect / Engineer:** Mark Byrne  This role is responsible for designing and configuring the cloud infrastructure. It also requires the configuration of the network and the connectivity with the on-site systems.  **Server Administrator:** Mauricio Guerra  This role requires the Server administrator to collaborate with the entire team and assist in the secure transition to the AWS and provide a smooth transition. |
| SUPPORT RESOURCES | During the course of the project, the team will require access to the necessary cloud platform resources, security tools and defense technologies, and communication platforms that ensure smooth communication to on-site technologies. |

**STAKEHOLDERS**

|  |  |
| --- | --- |
| OzCazual Management | OzCazual management has provided SecureNET with information about:   * the organizations current infrastructure limitations, * the process for migration of the current infrastructure to a cloud environment * their goals and requirement for scalability of future growth |
| SecureNET Management | SecureNET management are responsible for the oversight of the project, including the strategic decision makings and ensuring the project aligns with OzCazual’s goals and objectives. |
| AWS Cloud Service | Although they are not directly involved in the project, it is important to note that AWS is an important stakeholder. SecureNET will have to collaborate with AWS, to assure OzCazual that their infrastructure and services are running in a secure environment |
| Server Administrator | The server administrator with the SecureNET team will assist in the transition from the local infrastructure to the cloud environment. The server administrators will work closely with the SecureNET team and be large part of the project |
| IT Department | The internal IT department of OzCazual, who will work collaboratively with SecureNET, and provide them with any support during the project |
| Project Owner | The project owner Hettige Jayatissa who represents OzCazual, has the authority to make decisions and provide directions throughout the life of the project |
| End Users | All the staff of the OzCazual organization that will use the cloud environment daily |
| Customers | Employees of OzCazual’s e-commerce website, who will rely on the security of the infrastructure, to keep their information and transaction data secure. |
| Regulatory and Compliance Authorities | This stakeholder plays a significant role in assuring the migration process follows the security requirements and guidelines that need to be followed. Should this stakeholder perform audits, they can address specific requirements that need to be met |

Full stakeholders register available - “1.1 - Stakeholder Register - v1.0.docx”

**Information Sources**

|  |  |
| --- | --- |
| Project Charter | This outlines the project objectives, scope, stakeholders and high-level requirements |
| OzCazual Business Requirements | The management of OzCazual have expressed their requirement and concerns regarding the security of their cloud infrastructure, with the intent to meeting compliance standards specific to their industry |
| Systems Administrators | Information provided by the administrator of the existing local server infrastructure, the planned migration to the AWS cloud, and their specific requirements of the security for the cloud environment |
| Cyber Security Experts | As they are the experts in their respective fields, their expertise and industry knowledge will provide the specialized skills required for the migration and securing the cloud environment |
| Compliance Frameworks and Regulations | Depending on the need specific to OzCazual, there are industry-specific compliance frameworks and regulations that are required to be followed, such as PCI-DSS, HIPAA, or GDPR. Since OzCazual performs online transactions, there will be a requirement and compliance to follow |
| Amazon AWS Cloud Provider | Documentation and best practices provided by Amazon AWS regarding cloud security, recommended configurations, and available security features. |

**TENTATIVE SCHEDULE**

|  |  |  |
| --- | --- | --- |
|  | **PLANNED** | |
| **KEY MILESTONE** | **START** | **FINISH** |
| Project initialization and stakeholder alignment | 5th June, 2023 | 9th June, 2023 |
| Security assessment and risk analysis | 12th June, 2023 | 18th June, 2023 |
| Design and implement security systems and controls | 19th June, 2023 | 25th June, 2023 |
| Test and validate security controls | 26th June, 2023 | 2nd July, 2023 |
| Create comprehensive documentation | 3rd July, 2023 | 7th July, 2023 |
| Provide training documentation | 3rd July, 2023 | 7th July, 2023 |
| Finalize all project activities | 8th July, 2023 | 10th July, 2023 |
| Conduct a final review and presentation | 8th July, 2023 | 12th July, 2023 |
| Prepare final hand-over documentation | 12th July, 2023 | 14th July, 2023 |

**COSTS**

|  |  |
| --- | --- |
| The projected budget for the AWS CyberShift Initiative, is projected to be in the amount of $40,000.  This will cover all aspects of the project's costs, including the acquisition of new equipment, software licenses, and external services such as the AWS cloud environment.  The breakdown is as follows: | |
| **COST** | **DESCRIPTION** |
| **Personnel** | This includes the cost of project personnel, such as cybersecurity specialists, system administrators, cyber security engineers, project managers.  Each member of the team is estimated to be $150 per hour |
| **Equipment Acquisition** | For the purchase or upgrade of hardware and software components, required for securing the cloud infrastructure, and upgrading the local infrastructure to communicate smoothly and securely with the cloud environment. |
| **Software Licenses** | This cost includes acquiring software licenses for anti-virus/malware security, vulnerability scanning software, or other relevant software. |
| **External Services** | This covers the cost of external services such as penetration testing, security audits or third-party consultants. |

**RISKS, CONSTRAINTS, AND ASSUMPTIONS**

|  |  |
| --- | --- |
| **RISKS** | * There is a risk of a data breach, resulting in unauthorized access to the cloud infrastructure, if the cloud environment is not properly secured. If this should happen, there could be a risk of sensitive information being accessed, leading to damage of the company reputation and the loss in trust of its customers * Should OzCazual have employees that have inadequate expertise in Cyber defense, the risk of inadequate security measures or response could lead to a significant breach * There could be a failure to comply with the industry security standard and/or regulations, that could result in hefty penalties, legal consequences, or damage to the company’s reputation * There could be integration and migration issues with the existing systems and applications that could require forced downtime to successfully migrate to the cloud environment, resulting in operational disruptions. * The AWS cloud service could experience downtime or performance issues that are outside of OzCazual or SecureNET’s control, causing disruptions in the services provided be OzCazual |
| **CONSTRAINTS** | * Whether the chosen security controls, including 2FA, should be compatible with the cloud infrastructure and technology stack * Since the project must operate within the specific budget, restraints could limit the type of security measures that could be implemented * Operating on a specific timeline with deadlines in place could restrict the amount of time given on any specific task, such as the amount of time spent on penetration testing. Therefore, time will need to be managed carefully, to allow the implementation and testing of security measures * Depending on the level of expertise, it could allow for certain vulnerabilities to exist if the skill level of the cyber security team is unable to detect them during testing and analysis of the implemented security measures |
| **ASSUMPTIONS** | * The successful execution of the project is conditional in the assumption that the management of OzCazual is fully supportive of the necessary resources required to complete and execute the project * If users will have access to a device (e.g., smartphone) that is required for an SMS method of 2FA * It is assumed that the AWS service will have the necessary resources and infrastructure required to migrate the existing local network to the cloud environment. It's also assumed AWS has the required hardware, network connectivity, and cloud service subscriptions to provide OzCazual with adequate availability. * The team of SecureNET specialists, consisting of the Project Manager, Cyber Engineer, Cloud Specialist, Systems administrator, and other stakeholders, will communicate effectively to ensure smooth execution of the project |

|  |  |  |
| --- | --- | --- |
| PREPARED BY | TITLE | DATE |
| Giuseppe Raciti | Project Manager | 13/06/2023 |