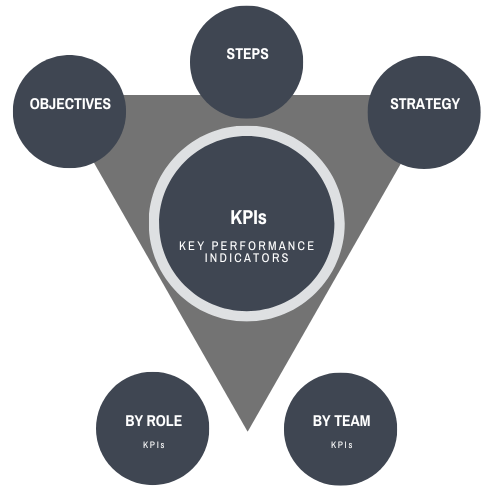
| **I) Key Performance Indicators (KPIs)** | |
| --- | --- |

In order to understand the Key Performance Indicators for the OZCasual’s server migration to AWS Cloud we require a comprehensive approach of what strategies, steps and objectives are relevant. In that way we can ensure the confidentiality, integrity, and availability of their data.



The following scope provides the key aspects of the OZCasual’s migration process based in the precious objectives, steps and strategies:

1. **Infrastructure Assessment:** Assess the existing server infrastructure in order to identify potential security vulnerabilities and areas of improvement.
2. **Security Architecture Design:** Develop the security architecture for the AWS Cloud, including network segmentation, access control, encryption, and monitoring.
3. **Data Migration Planning:** Includes different variables: data sensitivity, compliance requirements, secure data transfer mechanisms and encryption.
4. **Security Monitoring and Incident Response:** Set up security monitoring tools and configure logging to detect in order to respond to security incidents.
5. **Backup and Recovery:** Implement AWS Cloud services, for example Amazon S3 for data backup and AWS Disaster Recovery services for recovery options.
6. **Compliance and Audit:** Ensure adherence to relevant industry regulations and compliance standards, such as HIPAA. Conduct regular audits and vulnerability assessments to maintain a secure environment.
7. **Security Optimization:** Monitor and optimize security controls, implementing regular security patches and updates.

| **II) KPIs for role** | |
| --- | --- |

| **Project Manager** - Giuseppe Raciti | |
| --- | --- |
| **Role Responsibilities:** | |
| Overall project coordination and management: | * Coordinate all project activities from initiation to closure * Ensures project resources are allocated effectively and efficiently * Monitors the progress of the project and take necessary actions to keep on track * Facilitates communications and collaboration amongst the team * Holds regular project status meetings to keep up-to-date |
| Plan, organize, and control project activities: | * Develops a project schedule with consideration of resources available * Defines the project deliverables, milestones and success criteria * Establishes project management methodologies and processes * Monitors and controls the project scope, schedule and budget * Conduct risk assessments and develop risk mitigation strategies * Manage project documentation and version control |
| Ensures project deliverables are completed on time and within budget: | * Monitor project progress against the defined schedule and budget * Identify potential deviations and take corrective actions * Manage change requests and assess their impact on project scope, schedule, and budget. * Collaborate with stakeholders to prioritize project activities and deliverables. * Ensure project resources are utilized effectively and efficiently. |
| Risk management and mitigation: | * Identify and assess project risks and develop mitigation plans. * Regularly review and update the risk register. * Monitor risk triggers and implement risk response strategies. * Facilitate risk workshops and discussions with the project team. * Escalate high-priority risks to relevant stakeholders |
| Stakeholder Communication and Reporting: | * Establish effective communication channels with stakeholders. * Provide regular project status updates to stakeholders. * Address stakeholder concerns and manage expectations. * Prepare and distribute project reports * Conduct project review meetings to gather feedback and ensure alignment with stakeholder requirements. |
| **Key Performance Indicators (KPIs):** | |
| Project is completed within the defined timeline: | * Measure the actual project duration against the planned timeline. * Calculate the variance between planned and actual completion dates.   **KPI target:** Project completed within the defined timeline |
| Ensure project remains within the allocated budget: | * Track project expenses and compare them to the allocated budget. * Monitor cost variances and take corrective actions if necessary.   **KPI target:** Project expenses within the allocated budget |
| Stakeholder satisfaction: | * Gather feedback from stakeholders regarding project deliverables and overall satisfaction. * Conduct stakeholder interviews to assess their satisfaction levels.   **KPI target:** Positive stakeholder satisfaction ratings based on feedback. |
| Team productivity and collaboration: | * Evaluate the team's performance in terms of meeting deadlines. * Assess the level of collaboration and teamwork within the project team.   **KPI target:** High productivity levels and positive team dynamics. |
| Effective risk management resolution: | * Evaluate the effectiveness of risk identification, mitigation, and response strategies. * Monitor the resolution of project issues and assess their impact on project performance.   **KPI target:** Proactive risk management and timely resolution of project issues. |

| **Cyber Security Specialist** - Shaun Heywood | |
| --- | --- |
| **Role Responsibilities:** | |
| Security Awareness Training | * Provide guidance on security best practices * Develop training materials, including presentations, videos and interactive modules to educate employees about security best practices. * Conducting training sessions in person or through virtual platforms to promote awareness of cybersecurity risks. * Assessing and monitoring the effectiveness of the training program using assesment, quizzes and surveys. |
| Documentation and policies | * Policy development and maintaining comprehensive cybersecurity policies and procedures that align with industry best practices * Documentation management, including creating and updating security documentation and security control frameworks * Policy enforcement and compliance for the effective communication to the employees and monitoring their adherence. |
| Conduct assessments of the existing infrastructure | * Monitor and analyze logs for potential security threats or breaches * Collaborate with the project team to address security vulnerabilities and risks |
| Security Infrastructure management | * Design and implement security measures for the cloud infrastructure * Configure and manage firewalls, IPS/IDS systems, and antivirus/malware protection * Configuring and maintaining security devices and tools, applying patches and updates |
| Incident response | * Detecting and analyzing security incidents, including breaches, malware infections, or unauthorized access attempts * Taking immediate action to contain the incident, minimize its impact, and prevent further spread of the threat * Documenting and reporting incidents to relevant stakeholders, coordinating with internal teams or external entities |
| **Key Performance Indicators (KPIs):** | |
| Security Vulnerability Assessment: | * Monitor the vulnerability assessments of the existing server infrastructure * Identify potential security weaknesses   **KPI target:** Identify the number of high-severity vulnerabilities and remediated |
| Security Incident Response Time | * Track the Cyber Security Specialist's ability to respond promptly to security incidents and breaches. * Minimize the time between detection and resolution. * Mitigation response to implement mitigation responses against attacks * Attack traffic identification, measuring the accuracy in order to identify malicious traffic   **KPI target:** Know the average time taken to detect and respond to security incidents |
| Compliance Adherence | * Monitor the compliance with relevant industry regulations and standards * Measure the adherence to HIPAA   **KPI target:** Percentage of compliance requirements met within given period |
| Security Controls Implementation | * Measure the implementation of encryption * Measure the implementation of access controls * Measure the implementation of IDS/IPS * Measure the implementation of Firewalls   **KPI target:** Number of security controls successfully deployed |
| Security Audits and Penetration Testing: | * Attack detection for DDoS, SSH, Malware protection * Downtime duration after an attack was done * Incident response evaluation   **KPI target:** Testing the critical vulnerabilities identified through the penetration testing process |

| **Cloud Architect/Engineer** - Mark Byrne | |
| --- | --- |
| **Role Responsibilities:** | |
| Cloud Infrastructure Design and Implementation | * Design and implement cloud infrastructure solutions that align with business requirements and industry best practices. * Conduct capacity planning, scalability assessment, and cost optimization for cloud resources. * Define and enforce security measures, access controls, and data protection mechanisms within the cloud environment. * Collaborate with stakeholders to gather requirements, provide technical expertise, and ensure successful deployment of cloud solutions. * Stay updated with emerging technologies, trends, and advancements in cloud computing. |
| Cloud Solution Architecture | * Collaborating with the Cyber Security Specialist to implement security measures * Develop and design architectural blueprints and solution roadmaps for cloud-based applications and services. * Ensure integration, interoperability, and compatibility of cloud solutions with existing systems and applications. * Define architectural patterns, standards, and best practices for cloud application development and deployment. * Conduct proof-of-concept evaluations and performance testing for cloud-based solutions. * Collaborate with development teams to provide guidance on architecture-related matters. |
| Cloud Migration and Optimization | * + Develop migration strategies and plans, including selecting appropriate migration tools and services.   + Optimize resource utilization, cost efficiency, and performance of cloud deployments through continuous monitoring and optimization techniques.   + Identify opportunities for workload consolidation, automation, and containerization in the cloud environment. |
| Cloud Governance and Compliance | * Define and enforce cloud governance frameworks, policies, and procedures. * Ensure compliance with industry standards, regulatory requirements, and data privacy regulations. * Establish monitoring and auditing mechanisms to track cloud resource usage, performance, and compliance. * Collaborate with legal, compliance, and risk management teams to address cloud-related compliance issues. |
| Cloud Consultation and Collaboration | * + Provide technical guidance, mentorship, and consultation to cross-functional teams and stakeholders.   + Collaborate with business leaders, project managers, and developers to align cloud solutions with organizational goals.   + Participate in architectural reviews, technology selection, and vendor evaluations for cloud-based initiatives.   + Assist in the evaluation and selection of cloud service providers and third-party solutions.   + Foster knowledge sharing, conduct training sessions, and contribute to the development of cloud-related documentation and best practices. |
| **Key Performance Indicators (KPIs):** | |
| Architecture Design | * Monitor the ability to design a secure, and highly available architecture for the migrated server infrastructure in the AWS Cloud. * Designing and configuring the cloud infrastructure on Amazon AWS * Providing technical expertise on cloud architecture and services   **KPI target:** Project completed with alignment of the implemented architecture with established security frameworks and industry best practices |
| Scalability | * Track the designing and implementation of a scalable infrastructure that can adapt to changes in demand * Ensuring scalability and high availability of the cloud environment * Measure the average response time of the system when subjected to varying levels of load * Assessing the ability of the architecture to handle increased traffic while maintaining optimal performance   **KPI target:** Measure the ratio of successfully scaled resources to the total number of scaling requests, indicating the effectiveness of scaling operations. |
| Resource Optimization | * Monitor the efficient use of compute, storage, and networking resources in the AWS Cloud * Monitoring and optimizing cloud infrastructure performance * Measure the cost savings achieved through effective resource allocation, utilization, and optimization strategies in the cloud architecture   **KPI target:** Project effectiveness of resource allocation processes to ensure optimal utilization and allocation of cloud resources |
| Availability and Disaster Recovery | * Monitor the design and implementation of high availability and disaster recovery mechanisms. For example automated AWS backups * Check the average time it takes to recover services and applications after a disruption or disaster * Measure the percentage of time that services and applications are available and operational   **KPI target:** Projectaverage time taken to restore services and applications to full functionality after a disruption or disaster |
| Cost Management | * Track the success in managing costs associated with the AWS Cloud infrastructure, optimizing resources and implementing cost-effective solutions * Measure the ratio of cost savings achieved through optimization strategies * Measure the accuracy of cost estimation and forecasting, ensuring that the actual costs align with the projected budget   **KPI target:** Project efficiency of resource utilization by evaluating the ratio of the value generated from cloud resources to the cost incurred |

| **Mauricio G. Guerra** - Server Administrator | |
| --- | --- |
| **Role Responsibilities:** | |
| Server maintenance | * Install and update operating systems, applications, and server software * Monitor server performance, troubleshoot issues, and optimize server resources |
| Server migration to AWS | * Collaborating with the project team to ensure a secure transition to AWS * Assisting in the migration of systems and data to the cloud environment * Providing technical assistance during the transition phase * Ensuring the smooth operation of the server infrastructure in the cloud environment |
| Server administration | * Configuring and managing the Windows Server 2019 Active Directory server * Supporting the setup and configuration of the Amazon Linux 2 web server |
| Server security | * Implement security controls and best practices to protect server infrastructure * Apply security patches, updates, and vulnerability management processes. |
| **Key Performance Indicators (KPIs):** | |
| Incident Response | * Monitor the ability to respond to server incidents * Minimize the time between incident detection and resolution.   **KPI target:** Project completed measuring the average time taken to resolve server-related incidents, including troubleshooting, diagnosing, and restoring server functionality |
| Server Uptime | * Monitor the ability to maintain the server uptime. * Confirming minimal downtime and maximizing availability to access to the server infrastructure   **KPI target:** Percentage of time that servers remain operational and accessible to users, indicating the reliability and availability of the server infrastructure |
| Backup and Recovery | * Monitor the design and implementation of high availability and disaster recovery mechanisms. For example automated AWS backups * Check the average time it takes to recover services and applications after a disruption or disaster * Measure the percentage of time that services and applications are available and operational   **KPI target:** Projectaverage time taken to restore services and applications to full functionality after a disruption or disaster |
| System Performance | * The ability to monitor and optimize server performance, including CPU, memory, disks, providing an efficient operation of the server infrastructure   **KPI target:** Measure the average time taken for the system to respond to user requests |
| Security Patching and Vulnerability Management | * Apply security patches and updates to the server infrastructure. * Check the percentage of systems and applications that are up-to-date with the latest patches and updates   **KPI target:** Know the average time taken to identify and remediate vulnerabilities in the cloud environment |

| **III) KPIs for the project team** | |
| --- | --- |
| Overall project completion within the defined timeline: | * Measure the actual project completion date against the planned timeline. * Identify any delays or schedule deviations and take necessary corrective actions. * Regularly monitor and update the project schedule to ensure timely delivery.   **KPI target:** Project completed within the defined timeline |
| Adherence to the allocated budget and resource utilization: | * Monitor project expenditures and compare them to the allocated budget. * Track resource utilization and ensure optimal allocation of resources. * Identify any cost overruns or budget deviations and implement corrective measures.   **KPI target:** Adherence to the allocated budget and efficient resource utilization |
| Stakeholder satisfaction with the project outcomes: | * Conduct stakeholder interviews for feedback to assess satisfaction. * Gather feedback on project deliverables, communication, and overall experience.   **KPI target:** High stakeholder satisfaction ratings based on feedback and evaluations. |
| Team productivity and collaboration: | * Evaluate individual and team productivity in completing assigned tasks and deliverables. * Assess collaboration and communication among team members. * Monitor team performance indicators, such as meeting deadlines and achieving milestones.   **KPI target:** High productivity levels and effective collaboration within the team. |
| Effective risk management and issue resolution: | * Identify and assess project risks regularly * Implement risk mitigation strategies and monitor risk triggers * Track the resolution of project issues and assess their impact on project performance * Address risks and issues in a timely manner to minimize their impact   **KPI target:** Proactive risk management, timely issue resolution, and mitigation effectiveness |
| Successful implementation of security measures: | * Ensure that the planned security measures are implemented effectively * Evaluate the deployment and configuration of security tools and technologies * Monitor the effectiveness of security controls and their impact on system security   **KPI target**: Successful implementation of security measures to protect the cloud infrastructure and data |
| Timely identification and resolution of security vulnerabilities: | * Regularly conduct security assessments and vulnerability scans * Promptly identify and assess security vulnerabilities and weaknesses * Implement appropriate remediation measures to address identified vulnerabilities   **KPI target:** Identification and resolution of security vulnerabilities to minimize the risk of exploitation |
| Efficient deployment and configuration of cloud infrastructure: | * Ensure the deployment of the cloud infrastructure components * Implement best practices for configuring the cloud environment   **KPI target:** Efficient and effective deployment and configuration of the cloud infrastructure |
| Adherence to cloud security best practices: | * Ensure compliance with industry standards and best practices for cloud security. * Regularly review and update security policies and procedures. * Monitor security controls and conduct audits   **KPI target:** Adherence to established cloud security best practices to safeguard the environment |
| Timely resolution of infrastructure and server-related issues: | * Monitor the performance and health of the infrastructure and servers * Identify and address any infrastructure or server-related issues promptly * Minimize downtime and ensure the availability of critical systems   **KPI target**: Resolution of infrastructure and server-related issues to maintain system stability and reliability |
| Minimize disruption to regular business operations: | * Plan and execute security measures with minimal impact on day-to-day business operations * Ensure that security enhancements and changes are rolled out smoothly * Communicate and coordinate with relevant stakeholders to minimize disruptions   **KPI target:** Minimal disruption to regular business operations during the implementation of security measures |
| Continuous improvement of security posture and cloud performance: | * Implement mechanisms for continuous monitoring and improvement of security * Regularly review security controls, processes, and incident response procedures * Seek opportunities to enhance the performance and efficiency of the cloud environment   **KPI target:** Continuous improvement of security posture and optimization of cloud performance |