Project: METAL SNAKE

Work Breakdown Structure (WBS)

Project Sponsor: Brendan Gasparin

Project Manager: Brendan Gasparin

Date of Project Approval: 14/08/2024

Commencement Date: 29/07/2024

Estimated Completion Date: 17/11/2024

Estimated Project Duration: 4 Months

Version: 1.0 (2024-08-20)

Executive Summary

The Work Breakdown Structure (WBS) breaks down the work of the project into manageable components, ensuring that all necessary tasks are identified, organized, and tracked. It ensures that nothing is overlooked and that all deliverables are accounted for.

Project Overview

This WBS represents the lifecycle of the project, ensuring that all necessary work is captured and organized in a hierarchical structure. It is designed to guide the project team through each phase, from initial planning to final deliverables and project closure.

Major Deliverables

The major deliverables for the project include completion of the planning and design phase, execution of project tasks, testing, deployment, ongoing monitoring and control activities, and formal project closure.

Key Objectives

- Break the project into manageable work packages.
- Ensure that all phases of the project are covered, from initiation to closure.
- Allocate resources effectively and monitor progress.
- Achieve successful project delivery within scope, time, and budget constraints.

Structure of the WBS

The WBS is structured into several phases, sub-phases, and key deliverables, which are each further broken down into smaller tasks. This structure ensures that all aspects of the project lifecycle are covered and that the project team can manage and monitor progress effectively.

Table of Contents

1. Project Initiation

1.1. Conduct Feasability Study

- Analyse the feasibility of the project.
- Conduct cost-benefit analysis.
- Begin a business case if the project is feasible and the benefits outweigh the costs, else cancel the project.

1.2. Stakeholder Engagement

- Identify and engage stakeholders.
- Develop initial stakeholder register with communication methods and frequencies.

1.3. Develop Preliminary Schedule

- Develop a basic schedule of project phases, subphases, and deliverables.

1.4. Develop Scope Statement

- Develop an initial, high-level scope statement for the project.

1.5. Develop Initial Risk Register

- Identify potential risks that could impact project initiation.
- Develop risk management strategies for each risk.

1.6. Develop Project Charter

- Define the project purpose and objectives.
- Identify key stakeholders and project team.
- Secure approval for the project to move forward.

1.7. Write a Project Manager Assignment Document

- Identify project objectives, deliverables, and responsibilities.
- Write a formal document appointing the project manager to the project.

1.8. Finalize the Business Case and Project Manager Assignment

- Finalize the business case to justify the project to stakeholders using the information from the other documents.
- Get approval from all necessary stakeholders. They should sign the project charter and project manager assignment documents.

2. Planning and Design Phase

2.1. Develop Scope Statement

- Refine the scope statement further.
- Identify project deliverables and boundaries.
- Document assumptions and constraints.

2.2. Develop Work Breakdown Structure (WBS)

- Break down project deliverables into smaller components.

2.3. Develop Project Schedule

- Create a detailed project schedule with timelines for all tasks.
- Define task dependencies and critical paths.

2.4. Requirements Documentation

- Gather and document detailed project requirements.

2.5. Resource Planning

- Identify and allocate resources.
- Develop a resource plan.

2.6. Cost Estimation and Budgeting

- Estimate costs for all work packages.
- Finalize the project budget.

2.7. Risk Management Planning

- Identify and analyse risks.
- Develop risk mitigation and contingency plans.

2.8. Technical Specifications Development

- Develop detailed technical specifications for project deliverables.

2.9. Quality Management Planning

- Define quality standards and develop quality assurance processes.

2.10. Change Management Planning

- Develop a process for handling project changes.

2.11. Communications Planning

- Develop a communications management plan.
- Identify key communication methods and frequencies.

2.12. Project Plan

- Compile necessary information into the project plan.

3. Project Execution

3.1. Team Mobilization and Kick-off

- Assemble project team and conduct kick-off meeting.

3.2. Task Execution

3.2.1. Build Raspberry Pi Server

- Create and maintain technical documentation on the Raspberry Pi server
- Construct the Raspberry Pi.
- Install and configure OS.
- Install and configure https://brendangasparin.com
- Develop operating manual.

3.2.2. Build Cloud Server

- Create and maintain technical documentation on the cloud server.
- Construct the Raspberry Pi.
- Install and configure OS.
- Install and configure LAMP stack.
- Install and configure test WordPress site.
- Develop operating manual.

3.2.3. Build Raspberry Pi Firewall

- Create and maintain technical documentation on the Raspberry Pi firewall
- Construct the Raspberry Pi.
- Install and configure pfSense.
- Develop operating manual.

3.2.4. Build Raspberry Pi Router

- Create and maintain technical documentation on the Raspberry Pi router
- Construct the Raspberry Pi.
- Install and configure OpenWRT.
- Develop operating manual.

3.2.5. Build Raspberry Pi Wireless Access Point

- Create and maintain technical documentation on the Raspberry Pi WAP.
- Construct the Raspberry Pi.
- Research best OS to use for wireless access point.
- Install and configure OS.
- Configure wireless access point and wireless networks.
- Develop operating manual.

3.2.6. Integrate System Components into a LAN

- Create and maintain technical documentation on the overall system.
- Setup and configure the LAN.
- Develop operating manual.

3.2.7. Build SIEM System

- Create and maintain technical documentation on the SIEM system.
- Setup the cloud server instance.
- Install an appropriate OS and configure it.
- Install and configure a SIEM system.
- Develop operating manual.

3.2.8. Mautic Installation

- Create and maintain technical documentation on the Mautic system.
- Install Mautic on the Raspberry Pi server.
- Configure Mautic.
- Develop operating manual.

3.3. Quality Assurance

- Implement quality assurance processes to ensure deliverables meet standards.

3.4. Resource Management

- Manage resources to ensure that tasks are completed on time and within budget.

3.5. Risk Mitigation

- Implement risk mitigation strategies as risks are identified.

3.6. Change Management

- Handle change requests and update project plans as necessary.

3.8. Stakeholder Communication

- Provide regular updates to the stakeholders according to the communications plan.

4. Testing

4.1 Test Planning

4.1.1 Define Testing Objectives

- Clarify the scope and objectives of the testing phase (e.g., ensuring stability, security, and performance).

4.1.2 Develop Testing Strategy

- Create a testing strategy, specifying the types of tests to be performed (e.g., functional testing, security testing, performance testing).

4.1.3 Develop Test Plan

- Define the schedule, resources, tools, and personnel needed for testing.
- Document the success criteria for each test.

4.1.4 Set Up Test Environment

- Prepare the testing environment, including setting up test users, creating test data, and configuring testing tools.

4.1.5 Identify Test Cases

- Develop a comprehensive list of test cases covering all components of the infrastructure.

4.2 Functional Testing

4.2.1 Test Raspberry Pi Router

4.2.1.1 Connectivity Tests

- Ensure the router is correctly connected to the ISP modem and provides Internet access.
- Test bridged mode configuration.

4.2.1.2 DHCP and Static IP Tests

- Test the router's ability to assign IP addresses dynamically.
- Test static IP configurations for connected devices.

4.2.2 Test Firewall Raspberry Pi

4.2.2.1 Firewall Rule Validation

- Verify that firewall rules are properly configured and enforce security policies.

4.2.2.2 Intrusion Detection System (IDS) Tests

- Test the firewall's ability to detect and log intrusion attempts.

4.2.3 Test Network Switch

4.2.3.1 Port Configuration Testing

- Test that all Ethernet ports are functional and correctly configured.
- Verify VLAN setups if applicable.

4.2.4 Test Raspberry Pi Wireless Access Point

4.2.4.1 Wi-Fi Connectivity Tests

- Test the ability of Wi-Fi devices to connect to the network and access the Internet.

4.2.4.2 Wireless Security Tests

- Verify WPA2/WPA3 security configurations.

4.2.5 Test LAMP Stack Web Server

4.2.5.1 Web Server Functionality Tests

- Test the functionality of Apache, MySQL, PHP, and the web applications hosted on the server.

4.2.5.2 Database Connectivity Tests

- Ensure the MySQL database is accessible and functions correctly.

4.2.5.3 Mautic Email Automation Tests

- Test Mautic installation, ensuring that email campaigns and automation workflows function as expected.

4.2.6 Test Cloud-Based Web Server

4.2.6.1 Uptime and Failover Tests

- Simulate on-premises Internet outages and verify that the cloud-based server remains operational for hosting client websites.

4.2.7 Test SIEM System

4.2.7.1 Log Aggregation and Correlation Tests

- Verify that the SIEM system is correctly aggregating logs from the on-premises network.

4.2.7.2 Alerting and Notification Tests

- Ensure the SIEM system is generating alerts for suspicious activities and sending notifications to the appropriate personnel.

4.3 Performance Testing

4.3.1 Network Performance Testing

4.3.1.1 Bandwidth and Latency Testing

- Test network bandwidth and latency across all devices (e.g., router, switch, Wi-Fi access point).

4.3.1.2 Load Testing

- Simulate multiple users accessing the network and measure performance under load.

4.3.2 Server Performance Testing

4.3.2.1 Web Server Load Testing

- Simulate heavy traffic on the LAMP stack web server to measure response times and resource usage.

4.3.2.2 Database Load Testing

- Test the MySQL database under load to ensure it can handle multiple queries and large data sets efficiently.

4.3.3 Cloud Infrastructure Performance Testing

4.3.3.1 Cloud Web Server Performance Testing

- Measure the performance of the cloud web server under various traffic conditions.

4.4 Security Testing

4.4.1 Penetration Testing

- Conduct penetration tests on the on-premises network and cloud infrastructure to identify vulnerabilities.

4.4.2 Vulnerability Scanning

- Use automated tools to scan for vulnerabilities in the firewall, router, web server, and other critical components.

4.4.3 Security Configuration Audits

- Verify that all devices (e.g., router, firewall, web server) are configured securely and follow best practices.

4.4.4 SIEM System Security Testing

- Test the SIEM system's resilience to tampering and its ability to detect security breaches.

4.5 Backup and Recovery Testing

4.5.1 Backup Procedure Testing

- Test the regular backup procedures for the LAMP stack, Mautic, and other critical data.

4.5.2 Recovery Testing

- Simulate data loss scenarios and test the ability to restore systems from backups.

4.6 Documentation Testing

4.6.1 Test Technical Documentation

- Follow the technical documentation during testing to ensure that it accurately describes the installation and setup process.
- Identify any discrepancies or areas needing clarification.

4.6.2 Test Operating Manual

- Use the operating manual to perform routine tasks and maintenance activities.
- Verify that the manual provides clear instructions and identifies potential gaps or improvements.

4.7 User Acceptance Testing (UAT)

4.7.1 Staff Training and Feedback

- Train staff on the operation of the network and gather feedback on ease of use and documentation clarity.

4.7.2 Test End-User Experience

- Simulate typical end-user activities (e.g., connecting to Wi-Fi, accessing the web server) and gather feedback on performance and usability.

4.8 Test Reporting and Review

4.8.1 Test Summary Reports

- Document the results of all tests, including any issues identified and their severity.

4.8.2 Defect Tracking

- Log any defects or issues found during testing and track their resolution.

4.8.3 Test Review Meeting

- Conduct a meeting with stakeholders to review the testing results and decide on any further actions before deployment.

5. Deployment

5.1 Deployment Planning

5.1.1 Finalize Deployment Plan

- Review and finalize the deployment plan, including timelines, resources, and steps for deploying each component.

5.1.2 Risk Assessment

- Identify potential risks during deployment and prepare contingency plans.

5.1.3 Set Up Deployment Environment

- Ensure that the deployment environment (both on-premises and cloud) is ready for system migration.

5.2 Hardware Deployment

5.2.1 Deploy Raspberry Pi Router

- Install and configure the Raspberry Pi router in its permanent location.

5.2.2 Deploy Firewall Raspberry Pi

- Install the firewall Raspberry Pi, ensuring it's properly connected to the router and switch.

5.2.3 Deploy Network Switch

- Install and connect all necessary Ethernet devices to the network switch.

5.2.4 Deploy Raspberry Pi Wireless Access Point

- Install and configure the wireless access point for Wi-Fi connectivity.

5.3 Software Deployment

5.3.1 Deploy LAMP Stack Web Server

- Transfer the web server (including the LAMP stack and Mautic) from the test environment to the live environment.
- Configure DNS and SSL certificates.

5.3.2 Deploy Cloud-Based Web Server

- Deploy the cloud-based web server for client hosting and ensure it is fully operational.

5.3.3 Deploy SIEM System

- Set up the cloud-based SIEM system and configure it to start monitoring the on-premises infrastructure.

6.4 Data Migration

5.4.1 Backup Existing Data

- Perform a final backup of any existing data before the transition.

5.4.2 Migrate Data to New Systems

- Transfer any necessary data from the old infrastructure to the new servers.

5.4.3 Verify Data Integrity

- Ensure that all migrated data is intact and accessible on the new systems.

5.5 Security Configuration

5.5.1 Implement Final Security Policies

- Apply final security configurations, including firewall rules, encryption settings, and access controls.

5.5.2 Conduct Post-Deployment Security Audit

- Perform a security audit to ensure that the deployed systems meet all security requirements.

5.6 Testing and Validation

5.6.1 System Functionality Tests

- Test all systems (network, servers, SIEM) to ensure they are functioning as expected in the live environment.

5.6.2 User Acceptance Testing

- Allow users (business and residential) to test the network and web services, ensuring they meet operational requirements.

5.6.3 Final Performance Testing

- Conduct performance tests to ensure the systems can handle live traffic and load.

5.7 Training and Handover

5.7.1 Staff Training

- Train staff on operating and maintaining the newly deployed systems.

5.7.2 Handover to Operations

- Officially hand over the deployed systems to the operations team for ongoing management and monitoring.

5.8 Documentation and Reporting

5.8.1 Update Documentation

- Update all technical and operational documentation to reflect the deployed environment.

5.8.2 Deployment Report

- Prepare a report summarizing the deployment process, including any issues encountered and resolutions.

6. Closure and Maintenance

6.1. Final Deliverable Handover

- Complete and deliver final project deliverables to all stakeholders.

6.2. Project Review and Evaluation

- Conduct a post-project review to evaluate project success.
- Document lessons learned.

6.3. Stakeholder Sign-Off

- Obtain formal approval and sign-off from stakeholders.

6.4. Close Contracts

- Complete and close all project-related contracts.

6.5. Archive Project Documentation

- Organize and archive all project documentation for future reference.

6.6. Celebrate Success

- Celebrate project completion with the team.

6.7. Transition to Operations

- Ensure a smooth handover of the project deliverables to the operations team.