Project: METAL SNAKE

Business Case

Project Sponsor: Brendan Gasparin

Project Manager: Brendan Gasparin

Date of Project Approval:

Commencement Date: 29/07/2024

Estimated Completion Date: 17/11/2024

Estimated Project Duration: 4 Months

Version: 1.0 (2024-08-12)

1. Executive Summary

1.1 Introduction

Project: METAL SNAKE is designed to reduce operational costs, improve service delivery for clients, and enhance the organization's cybersecurity posture. This business case outlines the strategic objectives, benefits, and implementation plan for the project, highlighting its critical role in achieving organizational goals.

1.1. Project Objectives

- Reduce cloud server costs by over 50%, leading to significant operational savings.
- Implement scalable and reliable infrastructure to support client services.
- Improve cybersecurity measures to protect client data, enhance trust, preserve reputation, and avoid costly legal fines associated with data breaches.
- Provide staff facilities for cybersecurity training, improving organizational knowledge.

1.2. Project Overview

Project: METAL SNAKE is the construction of an on-premises cybersecurity lab with a server for hosting business infrastructure and the organization's website. It also includes the provision of cloud servers for hosting client websites, to avoid any downtime caused by faulty residential Internet.

METAL SNAKE will also include a cloud-based SIEM security system for improved security posture, organizational knowledge, and employee training in cybersecurity.

The importance of METAL SNAKE is largely in reducing operational costs of cloud server hosting, but it will allow the organization to meet strategic goals of providing cost-effective Internet solutions to clients, driving innovation, and improving detection and response of cybersecurity incidents.

1.3. Key Benefits

- **Cost savings:** Projected annual savings of AUD 720 from reduced server costs.
- **Operational efficiency:** Streamlined processes resulting in 10% reduction in development time.
- **Risk mitigation:** Enhanced security measures to prevent data breaches and associated costs of AUD 10,000 to AUD 100,000 per breach.

1.4. Cost-Benefit Analysis Summary

The included cost-benefit analysis demonstrates a positive net present value (NPV) for Project: METAL SNAKE, indicating that the expected benefits significantly outweigh projected costs. The project is financially viable and strategically beneficial.

1.5 Risk Assessment

Major risks associated with the project and their mitigation plans include:

- **Budget Overrun:** A $500 contingency budget is being held in reserve for response to unexpected expenses.
- **Cybersecurity Threats:** Mitigated through the deployment of advanced security protocols and continued monitoring

1.6 Implementation Strategy

Project: METAL SNAKE will be executed over a 12-month period, with key phasings including planning and design, execution, testing, deployment, and maintenance. Adequate resources have been allocated to ensure timely and successful implementation.

1.7. Recommendations

It is recommended to proceed with Project: METAL SNAKE in order to gain the benefits of cost savings on cloud server hosting, optimizing resource allocation, improving operational efficiency, and enhancing cybersecurity capabilities of the organization.

The project aligns with our strategic objectives and offers significant financial and strategic benefits.

1.8. Conclusion

Project: METAL SNAKE is an important initiative that will drive significant improvements in cost management, operational efficiency, and cybersecurity capabilities. By implementing this project, the organization positions itself for sustained growth and success in an increasingly competitive landscape.

Table of Contents

2. Project Background

The organization is a web development agency that builds and intends to host websites for clients.

In the 2023-2024 fiscal year, the owner tried unsuccessfully to run a startup web development business called Cyborg Platypus. With difficulty getting clients and a diminishing budget, the owner decided in 2024 that it would be necessary to cut server costs.

Project: METAL SNAKE is the construction of an on-premises cybersecurity lab with a web server for hosting business infrastructure, plus a cloud server for hosting client websites and a cloud-based Systems Information and Event Management (SIEM) system for improved security posture, enhanced threat detection, and organizational training and knowledge in cybersecurity.

This will allow the business to cut the running costs of the existing cloud instance used to host business infrastructure and client websites, while also providing new opportunities in the field of cybersecurity.

2.1. Problem Statement

The organization is not making enough recurring revenue from web development or hosting to justify the cost of a $AUD100+/mo Google Cloud virtual instance without burning through the runway of the long-term budget. Over time, this virtual instance server and its costs will sink the business.

2.2. Analysis of Options

The following options have been considered to solve the problem:

1. Do nothing. Continue to pay $AUD90+/mo for the machine on Google Cloud. Unless massive market growth is achieved very quickly, the business will continue to haemorrhage this cost. The owner will eventually run out of capital or the desire to continue the business and it will fail.

2. Downgrade the Google Cloud server. This will save money, but the organization will lose automated email marketing capability and the ability to implement and run other computationally heavy operations in the future.

3. Drastically and quickly improve sales. If this is possible, it should be done regardless of server costs. But the business consists of one person who is inexperienced in sales and marketing, and growth in the short-term future is likely to be slow.

4. Implement a secure network with a dedicated web server on the business premises. Use an on-premises server for the business website, automated email marketing, and any future research, development, and implementation of software. Continue to use a less powerful, less expensive cloud virtual machine instance to host client websites, avoiding any client downtime caused by Internet outages on the business premises.

2.3. Recommended Option

Implementation of a secure network with a dedicated web server on the business premises and smaller cloud servers for website hosting and a SIEM offer many advantages.

- Cheaper running costs than hosting existing virtual machine instances on paid cloud services.
- Ability to directly access hardware for upgrades and installation of software and services.

- Organizational knowledge gained through practicing hardware installation, software installation, and best cybersecurity practices in an on-premises lab.
- Flexibility to continue running client websites on cloud server instances.

Therefore, implementation of a secure network on premises with 24/7 server applications, and cloud-based client website hosting, monitored by a SIEM cybersecurity system, is the recommended course of action for dealing with this problem.

3. Project Description

Project: METAL SNAKE will involve the planning, design, and implementation of a cybersecurity lab network with capabilities for hosting a LAMP stack web server and other services. This will involve both hardware and software installation on-premises, and installation of a SIEM system and another LAMP-stack web server in the cloud.

3.1. Project Objectives

The project has the following objectives:

1. Develop a secure network for running the organization and hosting Internet services.
2. Develop cloud servers for hosting client websites and a SIEM cybersecurity system.
3. Thorough documentation of the project for transparency, attracting employers and clients, and to add to the body of organizational knowledge.

3.2. Project Scope

The following features and functionality are in scope:

1. Installation of a home cybersecurity laboratory.
2. Installation of an on-premises web server to host organizational websites and services.
3. Installation of two cloud server instances: one for a LAMP stack web server to host client websites, and one for a SIEM system.
4. Documentation of each phase and sub-phase of the project.

3.3. Project Deliverables

The following deliverables can be expected from the project:

1. Customer router, firewall, server machine, and wireless access points.
2. A LAMP stack web server on the premises for cheaply hosting business infrastructure.
3. A cloud-based LAMP stack web server for hosting client websites.
4. A cloud-based SIEM system for monitoring cybersecurity events in the systems.
5. Documentation (including video) to showcase the project to future employers and clients.

3.4. Assumptions

1. The planned architecture and software can fulfill the deliverables of the project.
2. The organization will be able to continue to rent premises to house server hardware.

3.5 Constraints

1. Stakeholders will not tolerate lengthy outages to their Internet.
2. Budget is tight beyond what has already been assigned to pre-purchased hardware.
3. Documentation must redact all personal information (except the business owner's).

4. Stakeholder Analysis

4.1. Key Stakeholders

The following key stakeholders will be vital to the success of the project:

Stakeholder	Organisation	Role in Organisation	Interest in Project
Brendan Gasparin	Brendan Gasparin	Owner	Owner
[redacted]	Gasparin Family	Property Owner	Property Owner
[redacted]	Gasparin Family	Property Owner	Property Owner
[redacted]	Brendan Gasparin	Intern	Experience, fun
Clients	N/A	N/A	Web services
Users	N/A	N/A	Internet services

4.2. Stakeholder Needs and Expectations

Stakeholder needs and expectations are recorded below:

Stakeholder	Needs	Expectations
Brendan Gasparin	Home network with server	Adherence to budget
[redacted]	Functioning home Internet	Very little outage in Internet
[redacted]	Functioning home Internet	Very little outage in Internet
[redacted]	Education and experience	Fun
Clients	Web design and hosting	Stable, fast services
Users	Internet services	Stable, fast services

4.3. Stakeholder Communication Plan

Preferred communication methods and styles for each key stakeholder:

Stakeholder	Preferred Contact Method	Contact Details	Frequency of Contact
Brendan Gasparin	N/A	N/A	N/A
[redacted]	In Person	N/A	Daily
[redacted]	In Person	N/A	Daily
[redacted]	Discord	[redacted]	Weekly
Clients	Social media, website	N/A	Weekly
Users	Social media, website	N/A	Weekly

5. Market Analysis

To determine the feasibility and potential profitability of the project, factors to consider include market conditions, customer needs, and the competitive landscape.

5.1. Industry Overview/Market Conditions

The web development and hosting industry supports millions of websites globally. Small and medium enterprises, not-for-profits, and individuals can all desire strong online presences, driving demand for reliable and affordable web hosting solutions.

Current trends in the industry include a move toward digital transformation for small and medium organizations, the increased prevalence of managed hosting services, and a growing awareness of cybersecurity threats pushing the need for secure web hosting environments.

5.2. Target Market

The target market for development and hosting services on Project: METAL SNAKE's server deliverables include small businesses, entrepreneurs, freelancers, and creatives who need reliable, cost-effective web hosting solutions to establish and maintain their online presence.

5.2.1. Target Market Demographics

Our primary demographics are entities (organizations or individuals) with 1-50 employees and covering various industries such as retail, services, and arts. The owners or entities are typically aged 25-55. Marketing will focus on those who understand the importance of an online presence.

5.2.2. Target Market Psychographics

Out target market values affordability, reliability, and excellent customer service. They prefer working with local providers who take the time to understand their specific needs and challenges.

5.3. Market Needs

Many small businesses and entrepreneurs require affordable, reliable web development and hosting solutions that offer excellent customer service and understand their specific needs.

Project: METAL SNAKE will address this by providing a reliable, cost-effective web hosting solution, tailored specifically for small businesses, entrepreneurs, and creatives who value bespoke websites and excellent customer service.

5.4. Market Size and Growth

There are millions of small businesses globally that require web development and hosting services. In Australia alone, based on recent statistics, there are approximately 2.59 million actively trading businesses, with 97.3% of these classified as small businesses. Around 36% of small businesses do not have a website, resulting in an estimated 906,577 small businesses without an online presence.

Figures for additional target groups such as entrepreneurs and creatives are difficult to obtain, but it can at least be assumed that the total target market exceeds 906,577 possible clients.

The market was expected to grow at a compound annual growth rate (CAGR) of 20.2% from 2023 to 2030, driven by the increasing number of small businesses establishing online presences, projecting even larger target market sizes in the future.

5.5. Competitive Analysis

Key competitors include established web hosting providers like GoDaddy, Crazy Domains, Wix, Squarespace, and others, as well as local managed web development and hosting providers.

We will offer personalized service, competitive pricing, and excellent customer support. Our potential weaknesses will include a limited initial size and ability to scale compared to larger providers.

The competitive advantage offered by Project: METAL SNAKE will be reduced costs and enhanced cybersecurity capabilities, which will then be leveraged by the business using personalized service, bespoke website customization, and a strong focus on local organizations and individuals.

5.6. Market Trends

Significant current trends in the market include the adoption of cloud hosting, the use of open-source software for web servers, and the rise of managed hosting services.

Regulatory trends include data protection regulations, such as GDPR. This highlights the importance of secure hosting environments and compliance with privacy standards.

Economic trends include the increasing market value for skilled hosting providers, and the affordability of hosting hardware and software making it more accessible to a wider audience.

5.7. SWOT Analysis

Strengths: Comprehensive documentation; technical skill and hands-on experience; cost-effective infrastructure; cheap or (currently) unpaid labour.

Weaknesses: Limited budget; office space restrictions; additional constraints may be enforced by stakeholders; learning curve for adopting the new technologies.

Opportunities: Discover new ways to leverage system; possibility of getting new and improved premises; better reusability of digital assets; growing demand for cybersecurity skills.

Threats: Unforeseen technical difficulties; potential hardware failures and other unforeseen costs; cancellation of project by stakeholders; movement to new premises could lead to project delays and other unforeseen ramifications; the rapid pace of technological change; potential market saturation; and competition from established web development businesses; residential Internet is unreliable; improper application of security practices could lead to cyberattacks on business and residential infrastructure.

6. Cost Estimate and Financial Analysis

Cost estimation, budget allocation, financial projections, and a cost-benefit analysis for Project: METAL SNAKE follow.

6.1. Cost Estimate

Cost Estimate for Project: METAL SNAKE			
Expense	**Type**	**Est. Cost**	**Running Total**
Raspberry Pi 5 B 8GB x 4	Hardware	538.00	538.00
Raspberry Pi 5 Power Supply x 4	Hardware	82.60	620.60
Raspberry Pi 5 Official Case x 2	Hardware	34.42	655.02
Argon NEO 5 Raspberry Pi Case x 2	Hardware	69.90	724.92
Raspberry Pi Active Cooler x 4	Hardware	34.44	759.36
Raspberry Pi Keyboard	Hardware	32.00	791.36
Raspberry Pi Mouse	Hardware	18.00	809.36
512GB SanDisk MiniSD Card x 4	Hardware	323.96	1,133.32
Micro HDMI Cable x 2	Hardware	15.10	1,148.42
Wireless Network Adapter x 2	Hardware	93.60	1,242.02
USB to Ethernet Adapter x 2	Hardware	39.98	1,282.00
External Storage 5TB	Hardware	189.00	1,471.00
LAN cables x 5	Hardware	14.99	1,485.99
		Grand Total	1,485.99

Recurring Costs (per month)		
Recurring Expense	**Start Date**	**Cost**
Office Supplies	29/07/2024	$20
Static IP Hire	29/07/2024	$10
Cloud Server #1	08/09/2024	$15
Cloud Server #2	12/10/2024	$15
	Grand Total	$60

6.2. Budget Allocation

Budget Allocation for Project: METAL SNAKE (4 Months)					
Category	**Item Description**	**Start Date**	**Est. Cost**	**Frequency**	**Total Cost**
Initial Setup Costs					
Hardware	Computers, network equipment	29/07/2024	$1,485.99	One-Time	$1,485.99
Software	Free open-source software	29/07/2024	$0.00	One-Time	$0.00
Operational Costs					
Internet	Static IP Address	29/07/2024	$10.00	Monthly	$40.00
Hosting	Web server cloud hosting fees		$15.00	Monthly	$45.00
	SIEM cloud hosting fees		$15.00	Monthly	$15.00
Personnel Costs					
Project Manager	Salary	29/07/2024	$0.00	Fortnightly	$0.00
Intern	Salary	29/07/2024	$0.00	Fortnightly	$0.00
Training Costs					
Self-Education	Self-Education	29/07/2024	$0.00	One-Time	$0.00
Training Costs	Intern Training	29/07/2024	$0.00	One-Time	$0.00
Miscellaneous Costs					
Office Supplies	General Office Supplies		$20.00	Monthly	$80.00
Contingency Fund					
Contingency	Reserve for unexpected expenses		$500.00	One-Time	$500.00
				Grand Total	$2,165.99

6.3. Financial Projections

6.3.1. Pricing Structure

Pricing Structure				
Service or Product	**Frequency**	**Revenue**	**COGS**	**Gross Profit**
Basic Website and Email Package				
Basic Website and Email Package: Development, Website Hosting, Domain Name Registration, 1 Email	One-Time	$999.95	$112.21	$887.74
Basic Website and Email Package Annual Renewal	Yearly	$149.95	$118.22	$31.73
Web Development				
Basic Wordpress Installation (DIY Web Design)	One-Time	$199.95	$0.00	$199.95
Basic Website Development (3-5 pages)	One-Time	$875.95	$0.00	$875.95
Maintenance and Support	Hourly	$49.95	$0.00	$49.95
Web Hosting				
Basic Website Hosting (Basic Static Website with 1GB Storage or Less)	Monthly	$9.95	$0.75	$9.20
Domain Name Services				
.com.au or .au Domain Name Registration & Maintenance (Year 1)	Yearly	$29.95	$9.55	$20.40
.com.au or .au Domain Name Registration & Maintenance (Year 2+)	Yearly	$29.95	$20.99	$8.96
.com Domain Registration & Maintenance (Year 1)	Yearly	$29.95	$16.98	$12.97

.com Domain Registration & Maintenance (Year 2+)	Yearly	$29.95	$23.99	$5.96
Other Domain Suffix Registration & Maintenance	Yearly	Varies	Varies	Varies
Email Services				
Google Workspace Business Starter Email Setup & Maintenance (1 Email)	Yearly	$119.95	$93.48	$26.47
Consultant Fees				
Consultant Fees	Hourly	$49.95	$0.00	$49.95

6.3.2. Revenue Projections

The following projections are based off an estimate of delivering one Basic Package per month from October 2024 to June 2025.

Revenue Projection (Jul 2024 - Jun 2025)				
Month	**Basic Package Clients**	**Basic Package Revenue**	**Basic Package COGS**	**Basic Package Gross Profit**
Jul-24	0	$995.95	$112.21	$883.74
Aug-24	0	$995.95	$112.21	$883.74
Sep-24	0	$995.95	$112.21	$883.74
Oct-24	1	$995.95	$112.21	$883.74
Nov-24	1	$995.95	$112.21	$883.74
Dec-24	1	$995.95	$112.21	$883.74
Jan-25	1	$995.95	$112.21	$883.74
Feb-25	1	$995.95	$112.21	$883.74
Mar-25	1	$995.95	$112.21	$883.74
Apr-25	1	$995.95	$112.21	$883.74
May-25	1	$995.95	$112.21	$883.74
Jun-25	1	$995.95	$112.21	$883.74
	Total:	$11,951.40	$1,346.52	$10,604.88

6.3.3. Cost Projection

Cost Projection					
Cost Category	**Item Description**	**Unit Cost**	**Quantity**	**Frequency**	**Total Cost**
Initial Setup Costs					
Hardware	Equipment	1485.99	1	One-Time	1485.99
Software	OS and Tools	$0	1	One-Time	$0
Operational Costs					
Static IP	Static IP Hire	$10		Monthly	$120
Hosting	Cloud hosting fees	$15	1	Monthly	$180
Hosting	SIEM hosting fees	$15	1	Monthly	$180
Personnel Costs					
Project Manager	Salary	$0	1	Fortnightly	$0
Intern	Salary	$0	1	Fortnightly	$0
Miscellaneous					
Office Supplies	Office Supplies	$20	1	Monthly	$240
				Total	2205.99

6.3.4. Profit and Loss Statement (Income Statement)

Profit & Loss Statement	
Category	**Amount**
Revenue	
Basic Package	$11,951.40
Total Revenue	$11,951.40
Cost of Goods Sold	
Hardware	$1,485.99
WordPress All-in-One Migration	$105.80
Basic Package COGS	$1,346.52
Total COGS	$2,938.31
Gross Profit	$9,013.09
Operating Expenses	
Static IP Hire	$120.00
Cloud Instances	$360.00
Mobile Phone Plan	$420.00
Office Supplies	$240.00
Total Operating Expenses	$1,140.00
Operating Income	$7,873.09
Interest and Taxes	
Taxes	$1,338.43
Total Taxes and Interest	$1,338.43
Net Income	$6,534.66

6.3.5. Cash Flow Projection

Cash Flow Projection for Project: METAL SNAKE					
Month	**Cash Inflow**	**Cash Outflow**	**Net Cash Flow**	**Opening Cash Balance**	**Closing Cash Balance**
Jul-24	$0.00	$1,515.99	-$1,515.99	$2,165.99	$650.00
Aug-24	$0.00	$30.00	-$30.00	$650.00	$620.00
Sep-24	$0.00	$45.00	-$45.00	$620.00	$575.00
Oct-24	$999.95	$172.21	$827.74	$575.00	$1,402.74
Nov-24	$999.95	$172.21	$827.74	$1,402.74	$2,230.48
Dec-24	$999.95	$172.21	$827.74	$2,230.48	$3,058.22
Jan-25	$999.95	$172.21	$827.74	$3,058.22	$3,885.96
Feb-25	$999.95	$172.21	$827.74	$3,885.96	$4,713.70
Mar-25	$999.95	$172.21	$827.74	$4,713.70	$5,541.44
Apr-25	$999.95	$172.21	$827.74	$5,541.44	$6,369.18
May-25	$999.95	$172.21	$827.74	$6,369.18	$7,196.92
Jun-25	$999.95	$172.21	$827.74	$7,196.92	$8,024.66

6.3.6. Break-Even Analysis

A break-even analysis was performed for sales of the Basic Package. It suggests that the break-even point for Project: METAL SNAKE is 3 clients, or 3 sales of the Basic Package

Break-Even Analysis for Basic Package (2024-2025	
Fixed Costs (per year)	
Hardware and software	$1,591.79
Static IP Hire	$120.00
Cloud Instances	$360.00
Mobile Phone Recharges	$420.00
Total	$2,491.79
Variable Costs	
COGS	$112.21
Total	$112.21
Individual Sales Prices	$999.95
Break-Even Point	2.81

6.4. Cost-Benefit Analysis

6.4.1. Introduction

The cost-benefit analysis for Project: METAL SNAKE evaluates the financial viability of the project by comparing anticipated costs and benefits over a one-year period. This will determine whether the project should succeed and highlight the strategic value it offers to the organization.

6.4.2. Cost-Benefit Analysis Table

Cost-Benefit Analysis for Project: METAL SNAKE (1 Year Period)			
Costs		**Benefits**	
Category	**Cost/Year**	**Category**	**Worth**
Direct Costs		Cloud Hosting Savings	$780.00
Hardware	1485.99	Data Breach Prevention	$10,000.00
Software	105.8	Improved Server Uptime	$1,000.00
COGS	1346.52	Secure Email Hosting	$500.00
Total	2938.31	Increase project completion by 10%	$1,000.00
		10% Less Security Incidents	$500.00
		Total	$13,780.00
		Net Present Value (Year One):	$10,325.42

While some of these benefits may seem high, such as data breach prevention, they are based on industry standards of an organization running at full capacity. For example, a data breach may result in financial penalties ranging from AUD 10,000 to AUD 100,000. This cost-benefit analysis assumes the project infrastructure will prevent one breach a year, and the low average cost of such a breach has been added to the benefit of “Data Breach Prevention.”

Another benefit that has been quantified strangely is improved server uptime. The organization currently has no clients and would not benefit from improved cloud server uptime. But given time, sales, and an increased number of clients, these benefits may be properly realized. They have been calculated according to the revenue projection given above.

These benefits align directly with organizational goals of providing cost-affordable and customizable website, domain, and email hosting to clients, as well as organizational cybersecurity goals.

6.4.3. Qualitative Analysis

A qualitative analysis of Project: METAL SNAKE includes benefits that are difficult to quantify, such as improved brand reputation, customer satisfaction, and stakeholder and employee morale.

Another consideration is alignment with organizational strategic goals and objectives. By aligning the project with the desire to develop new technologies and possibly expand into cybersecurity we meet strategic goals for expansion and innovation.

7. Benefits Realization

7.1. Expected Benefits

The expected benefits of the project are the following:

1. **Reducing Cloud Server Costs:** from $105/month to $40/month (over 50%), allowing for competitive pricing and improved margins. This will result in an annual savings of AUD 780.
2. **Data Breach Prevention:** The cybersecurity lab and SIEM will prevent costly data breaches, preventing the need for data recovery, legal fees ranging from AUD 10,000 to 100,000 per breach, and reputational damage. Assuming prevention of one data breach per year, this will result in an estimated annual savings of approximately AUD 10,000.
3. **Improved Infrastructure for Hosting:** Implementing robust and scalable infrastructure for website hosting, ensuring high uptime, speed, and reliability for client websites. Assuming an increase from 98% to 99.9% uptime (72 hours per year), and a revenue impact of AUD 13.65 per hour saved, this could result in savings of AUD 982.20 annually.
4. **Continuous Improvement and Innovation:** in service delivery through innovation and adoption of new technologies using the new facilities and infrastructure. This is difficult to quantify but might result in a 5% increase in client retention with significant revenue implications.
5. **Integrating Advanced Security Features:** to protect client websites from cyber threats, enhancing trust and client satisfaction. An estimated 2-3% increase in client retention would lead to increased revenue.
6. **Comprehensive, Efficient, and Secure Email Hosting:** with features like spam filtering and custom domains. Savings from reduced spam and better performance could lead to productivity gains estimated at AUD 500-1,000 per employee annually.
7. **Streamlined Development Processes:** utilizing automation and improved workflows to reduce development time for websites and services. Assuming a 20% reduction in time spent on development tasks, 200 hours saved, and an hourly wage of $50/hour, this could result in an annual savings of AUD 10,000.
8. **Establishing Better Infrastructure for New Technological Development:** leading to faster technology development and increased competitiveness. A 10% increase in project completion rates is not unrealistic.
9. **Improved Training for Staff:** New infrastructure will allow for better investment in training for staff to enhance skills in web development, hosting, and cybersecurity. Better trained staff can be estimated to increase in productivity by 5%.
10. **Establishing a Cybersecurity Lab for Testing:** will allow for testing of new security solutions and improve internal security practices, indirectly benefiting client services. This is hard to quantify but the reduction in potential vulnerabilities should be significant.
11. **Improved Customer Support:** The overall infrastructure will allow for improved, reliable customer support and maintenance services, enhancing client relationships and loyalty. Enhanced customer support can improve customer retention by 5-10%, leading to recurring revenue growth.
12. **Research into Customized Solutions:** Improved infrastructure will aid in research into customizable solutions to meet specific client needs, improving satisfaction and retention rates. Custom solutions can improve satisfaction rates by 5%, boosting long-term client relationships.

13. **Reduced Vulnerabilities and Proactive Detection:** Improved organizational security posture resulting in reduced vulnerabilities, security incidents, and proactive threat detection. Assuming a reduction in one potential security incident a year, this could result in a savings of AUD 10,000/year.
14. **Increased Operational Efficiency:** through automated security monitoring, reducing the need for manual oversight by employees. Automated systems would reduce the need for 20% of manual oversight hours, resulting in savings based on reduced hours and average wages (wages are currently zero).
15. **Faster Incident Response:** to security incidents, reducing downtime and minimizing the impact on operations. An assumption of 50% reduction in incident response times would lead to faster responses, minimizing business disruptions and potential losses.
16. **Reduction of Cybersecurity Insurance Premiums:** due to an improved security posture. An estimation of 10% reduction on current premiums is not unrealistic.
17. **Enhanced Compliance:** with industry regulations and standards, avoiding potential fines and penalties estimated at AUD 50,000 per incident.
18. **Audit Readiness:** through detailed logs and reports generated by the SIEM system, reducing audit times and costs (currently zero) by 20%.
19. **Strengthened Reputation:** with customers and partners by demonstrating a strong commitment to cybersecurity. A 5% increase in new clients due to improved reputation is not unrealistic.
20. **Competitive Differentiation:** by positioning the organization as a leader in security practices and high-performance hosting solutions. This could potentially increase market share by attracting new clients.
21. **Visibility and Control:** over network activities and potential threats allowing for more effective security management. Better control would reduce management overhead by 10%.

7.2. Benefits Measurement

Benefits will be measured in the following ways:

7.2.1. Benefit 1: Measurement of Cloud Server Cost Savings

Measurement Method:

- Monthly expenditure reports comparing actual server costs to projected costs.
- Financial statements reflecting the impact on overall margins.

Metrics:

- Monthly server cost tracking of cloud server expenses.
- Calculate cumulative savings at the end of each fiscal year.

Target:

- Achieve and maintain an annual savings of AUD 780 by reducing costs from 105 AUD/month to 40 AUD/month.

7.2.2. Benefit 2: Measurement of Data Breach Prevention

Measurement Method:

- Incident logs and security reports tracking attempted breaches and successful preventions.
- Financial analysis of avoided costs, including data recovery and legal expenses.

Metric:

- Number of breaches prevented. Track incidents detected and stopped by security systems.
- Cost Avoidance. Estimate avoided breach costs based on industry averages.

Target:

- Prevent at least one major breach annually, avoiding penalties ranging from AUD 10,000 to 100,000.

7.2.3. Benefit 3: Measurement of Infrastructure Uptime

Measurement Method:

- System uptime reports from monitoring tools
- Customer satisfaction surveys regarding service reliability.

Metrics:

- Uptime percentage, measured monthly, aiming for 99.9%.
- Downtime hours reduced, tracked in downtime hours annually.

Target:

- Maintain 99.9% uptime, reducing downtime by 72 hours annually, with a financial impact of approximately AUD 1,000 based on revenue projections.

7.2.4. Benefit 4: Measurement of Improvement and Innovation

Measurement Method:

- Track the introduction of new features and technologies.
- Client feedback and retention rates.

Metrics:

- Number of innovations implemented per year
- Client retention rate, monitored by the percentage increase in client retention.

Target:

- Implement at least two new innovations annually, aiming for a 5% increase in client retention.

7.2.5. Benefit 5: Measurement of Advanced Security Features

Measurement Method:

- Security audits and customer feedback.
- Incident response times and threat detection efficiency.

Metrics:

- Security incidents reduced compared to previous year.
- Customer satisfaction, measured in relation to security.

Target:

- Reduce security incidents by 10% annually, enhancing customer trust.

7.2.6. Benefit 6: Measurement of Efficient Email Hosting

Measurement Methods:

- Email system performance reports.
- Employee productivity assessments.

Metrics:

- Spam reduction, measured in decrease in spam incidents.
- Productivity gains estimated per employee.

Target:

- Improve productivity by AUD 500-1,000 per employee annually.

7.2.7. Benefit 7: Measurement of Streamlined Development Process

Measurement Method:

- Project completion times and resource allocation reports.
- Feedback from development team on process inefficiency.

Metrics:

- Development time reduced, measured in average project completion time.
- Resource utilization, measured in improvements to resource allocation.

Target:

- Achieve a 20% reduction in development time.

7.2.8. Benefit 8: Measurement of Better Infrastructure

Measurement Method:

- Rate of technology adoption and employee feedback on infrastructure.
- Improvement in project delivery timelines.

Metrics:

- Monitor usage and feedback on new infrastructure.
- Measure improvement in project delivery and completion rates.

Target:

- Improve project completion rates by 10% annually.

7.2.9. Benefit 9: Measurement of Improved Staff Training

Measurement Method:

- Employee skill assessments and training program evaluations.
- Productivity metrics before and after training.

Metrics:

- Track progress in skill assessments
- Measure productivity improvements post-training.

Target:

- Increase productivity by 5% following training initiatives.

7.2.10. Benefit 10: Measurement of Cybersecurity Lab for Testing and Research

Measurement Method:

- Reports on new security solutions tested and implemented.
- Incident logs showing reduced vulnerabilities.

Metrics:

- Count the number of new solutions tested annually.
- Measure decreases in identified vulnerabilities

Target:

- Test and implement at least three new security solutions annually.

7.2.11. Benefit 11: Measurement of Improved Customer Support

Measurement Method:

- Customer support response time logs and satisfaction surveys.
- Retention metrics related to support interactions.

Metrics:

- Track reduction in average response times.
- Measure customer satisfaction related to support services.

Target:

- Improve response time by 20% and increase customer satisfaction scores.

7.2.12. Benefit 12: Measurement of Research into Customizable Solutions

Measurement Method:

- Feedback on client-specific solutions and customization requests.
- Retention rates linked to customized services.

Metrics:

- Count the number of customized solutions delivered.
- Track client retention related to customization.

Target:

- Deliver 10 customized solutions annually, improving retention by 5%.

7.2.13. Benefit 13: Measurement of Reduced Vulnerabilities and Proactive Detection

Measurement Method:

- Vulnerability assessments using automated scanning tools, penetration testing, and manual reviews.
- Security incident monitoring and monthly analysis reports.

Metrics:

- Number of vulnerabilities detected and remediated.
- Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to incidents.

Target:

- Achieve a remediation rate of 90% of identified vulnerabilities within 30 days of detection.

7.2.14. Benefit 14: Measurement of Increased Operational Efficiency

Measurement Method:

- Automation impact assessments and workload distribution reports.
- Employee time-tracking for manual tasks.

Metrics:

- Track reduction in manual oversight hours.
- Measure efficiency gains from automation.

Target:

- Reduce manual oversight by 20%, translating to AUD 5,000 in savings annually (if employees were paid).

7.2.15. Benefit 15: Measurement of Faster Incident Response

Measurement Method:

- Incident response logs and recovery time metrics.
- Cost analysis of downtime and recovery efforts.

Metrics:

- Track reduction in average response times.
- Measure impact on downtime hours.

Target:

- Reduce incident response times by 50%, minimizing downtime costs by 30%.

7.2.16. Benefit 16: Measurement of Reduction to Insurance Premiums

Measurement Method:

- Insurance premium invoices and negotiation documentation.
- Annual reviews of security posture improvements.

Metrics:

- Track percentage reduction in insurance premiums.
- Monitor improvements in security ratings.

Target:

- Achieve a 10% reduction in cybersecurity insurance premiums.

7.2.17. Benefit 17: Measurement of Enhanced Compliance

Measurement Method:

- Compliance audit reports and regulatory assessments.
- Tracking of regulatory changes and adaptation.

Metrics:

- Measure increases in successful compliance audits.
- Track avoidance of compliance-related fines.

Target:

- Achieve 100% compliance audit success, avoiding AUD 10,000 to 100,000 in penalties.

7.2.18. Benefit 18: Measurement of Audit Readiness

Measurement Method:

- Audit preparation logs and documentation efficiency reports.
- Cost analysis of audit preparation efforts.

Metrics:

- Track reduction in time spent preparing for audits.
- Measure savings from efficient audit readiness.

Target:

- Reduce audit preparation time by 20%, saving AUD 3,000 annually.

7.2.19. Benefit 19: Measurement of Strengthened Reputation

Measurement Method:

- Brand perception surveys and customer testimonials.
- Tracking of new client acquisition linked to reputation improvements.

Metrics:

- Measure improvement in customer perception surveys.
- Track increase in clients citing reputation as a factor.

Target:

- Improve brand perception scores by 10%, increasing new client acquisition by 5%.

7.2.20. Benefit 20: Measurement of Competitive Differentiation

Measurement Method:

- Market analysis and competitor benchmarking.
- Revenue growth linked to differentiated offerings.

Metrics:

- Measure increases in market share due to differentiation.
- Track revenue growth linked to unique services.

Target:

- Increase market share by 3% and revenue growth by 10% annually.

7.2.21. Benefit 21: Measurement of Visibility and Control

Measurement Method:

- Network activity monitoring reports and control assessment metrics.
- Incident management reports and feedback from IT staff.

Metrics:

- Measure improvement in network activity oversight.
- Track reduction in unmanaged incidents.

Target:

- Enhance visibility.

7.3. Realization Plan

7.3.1. Benefits Realization Plan Overview

This realization plan aims to ensure the expected benefits are efficiently achieved through a structured approach. This plan details the actions, responsibilities, timelines, and resources necessary to realize each benefit.

7.3.2. Benefit-by-Benefit Action Plan

7.3.2.1. Benefit 1: Reducing Cloud Server Costs

Actions:

- Evaluate current server usage and costs.
- Research and select cost-effective cloud service providers.
- Develop a migration plan with minimal downtime.
- Migrate to more cost-effective on-premises server and cloud instances.

Timeline: Complete migration by 08/09/2024.

Responsibility: Project Manager.

Resources:

- Budget for new service subscriptions.

- Staff time for migration execution.

7.3.2.2. Benefit 2: Data Breach Prevention

Actions:

- Implement cybersecurity lab to test security solutions.
- Deploy and configure a SIEM system.
- Conduct regular security audits and updates.
- Provide security training to all employees.
- Create and test incident response procedures.

Timeline: Fully operational by 13/10/2024.

Responsibility: Project Sponsor.

Resources:

- Budget for cybersecurity tools and training.
- Staff time for audits and incident response.

7.3.2.3. Benefit 3: Improved Infrastructure for Hosting

Actions:

- Upgrade hosting infrastructure.
- Invest in redundant systems and backup solutions.
- Implement monitoring tools for issue and incident detection.
- Regularly test backup and failover systems.
- Optimize network performance by reviewing and enhancing network configurations.

Timeline: Full deployment by 03/11/2024.

Responsibility: Project Manager

Resources:

- Hosting equipment.
- New hardware and software for redundancy.
- Cloud services.
- SIEM monitoring software.

7.3.2.4. Benefit 4: Continuous Improvement and Innovation

Actions:

- Research new technologies and emerging trends.
- Test new tools and processes in a controlled environment.
- Roll out successful innovations across the organization.

Timeline: Ongoing, with major implementations by Q4 2025.

Responsibility: Project Sponsor.

Resources:

- Research and development budget.

- Staff time for pilot programs and feedback collection.

7.3.2.5. Benefit 5: Integrating Advanced Security Features

Actions:

- Evaluate existing security measures and identify gaps.
- Implement new security features like encryption and multi-factor authentication.
- Monitor security performance with regular reviews of security logs and reports.
- Collaborate with external experts for additional insights.

Timeline: Ongoing, with major implementations by Q4 2025.

Responsibility: Project Manager.

Resources:

- Security software and tools.
- Budget for external security consultants.

7.3.2.6. Benefit 6: Comprehensive, Efficient, and Secure Email Hosting

Actions:

- Enhance email security with spam filtering and (if possible) encryption.
- Ensure reliable and scalable provision of email services.
- Off custom domain email options to clients.
- Keep email systems up to date with the latest features.

Timeline: Implement by Q1 2025.

Responsibility: Project Sponsor.

Resources:

- Email server software and security tools.
- Staff time for IT support.

7.3.2.7. Benefit 7: Streamlined Development Processes

Actions:

- Document existing development workflows.
- Identify bottlenecks, analyze them, and remove inefficiencies.
- Use tools to automate repetitive tasks.
- Train developers in new tools and processes.

Timeline: Processes optimized by Q3 2025.

Responsibility: Project Sponsor

Resources:

- Automation software and tools.
- Training resources for development staff.

7.3.2.8. Benefit 8: Establishing Better Infrastructure for New Technological Development

Actions:

- Plan facility upgrades, designing better lab and office spaces.
- Purchase the latest technology and tools when possible.
- Implement ergonomic solutions, enhancing workspaces for employee comfort.
- Regularly evaluate facilities and infrastructure and make regular adjustments.

Timeline: Facilities upgraded by Q4 2025.

Responsibility: Project Sponsor.

Resources:

- Budget for equipment and renovations.
- Contractors and suppliers for upgrades.

7.3.2.9. Benefit 9: Improved Training for Staff

Actions:

- Assess current staff skills and identify skills gaps and areas for improvement.
- Create tailored training programs, sessions, and materials.
- Schedule regular sessions and implement ongoing training and development.
- Gather feedback to evaluate training effectiveness and adjust programs as necessary.

Timeline: Training programs in place by Q4 2025.

Responsibility: Project Sponsor.

Resources:

- Training budget and materials.
- External trainers or e-learning platforms.

7.3.2.10. Benefit 10: Establishing a Cybersecurity Lab for Testing

Actions:

- Plan, design, and set up the cybersecurity lab space.
- Purchase necessary hardware and software for testing.
- Regularly test new security solutions.
- Keep detailed records of test results and insights.

Timeline: Deployment by 27/10/2024.

Responsibility: Project Sponsor and Project Manager.

Resources:

- Lab equipment and security software.
- Budget for ongoing tests and experiments.

7.3.2.11. Benefit 11: Improved Customer Support

Actions:

- Evaluate existing customer service processes.
- Use new tools like CRM systems to streamline customer interactions.
- Set clear targets for response times and resolutions.

- Provide customer service training to all support personnel.

Timeline: Improvements made by Q2 2025.

Responsibility: Project Sponsor.

Resources:

- CRM software and support tools.
- Training resources for support staff.

7.3.2.12. Benefit 12: Research into Customizable Solutions

Actions:

- Conduct market research to identify client needs and preferences.
- Develop custom solutions by creating prototypes and piloting customizable offerings.
- Gather feedback from clients to refine offerings.
- Roll out widely accepted solutions to a broad audience.

Timeline: Initial solutions delivered by Q3 2025.

Responsibility: Project Sponsor.

Resources:

- Research budget and development tools.
- Staff time for product design and testing.

7.3.2.13. Benefit 13: Reduced Vulnerabilities and Proactive Detection

Actions:

- Conduct regular vulnerability assessments, scanning systems for potential vulnerabilities.
- Deploy threat detection tools for proactive threat detection.
- Use dashboards for real-time visibility of network activities.
- Train security team in the latest detection techniques.

Timeline: Proactive measures in place by Q2 2025.

Responsibility: Project Sponsor.

Resources:

- Threat detection software and monitoring tools.
- Training materials for security staff.

7.3.2.14. Benefit 14: Increased Operational Efficiency

Actions:

- Document current workflows and identify inefficiencies.
- Implement process automation, using software to automate manual tasks.
- Optimize resource allocation by ensuring resources are deployed effectively.
- Continuously monitor, assess, and refine operations for efficiency.

Timeline: Efficiency improvements implemented by Q3 2025.

Responsibility: Project Sponsor.

Resources:

- Automation tools and software.
- Process improvement resources.

7.3.2.15. Benefit 15: Faster Incident Response

Actions:

- Develop an incident response plan, creating and testing comprehensive response procedures.
- Deploy response tools to speed up detection and response times.
- Conduct simulations to regularly test response plans.
- Continuously review and improve response plans based on feedback.

Timeline: Incident response improvements by Q1 2025.

Responsibility: Project Sponsor.

Resources:

- Incident management tools and software.
- Budget for simulations and training.

7.3.2.16. Benefit 16: Reduction of Cybersecurity Insurance Premiums

Actions:

- Improve security measures by implementing advanced security protocols.
- Work with insurance providers to demonstrate improved security posture.
- Negotiate premiums by leveraging security improvements.
- Regularly review insurance policies.

Timeline: Premium reductions by Q4 2025.

Responsibility: Project Sponsor.

Resources:

- Insurance policy documents.
- Security audit reports.

7.3.2.17. Benefit 17: Enhanced Compliance

Actions:

- Conduct compliance audits, regularly assessing adherence to regulations and standards.
- Revise policies to ensure ongoing compliance.
- Train staff on compliance.
- Engage regulatory bodies with open communication.

Timeline: Full compliance by Q2 2025.

Responsibility: Project Sponsor.

Resources:

- Regulator guidance and resources.
- Training materials for staff.

7.3.2.18. Benefit 18: Audit Readiness

Actions:

- Prepare, organize, and maintain detailed records for audits.
- Conduct regular internal audits to assess readiness.
- Engage with external auditors for independent assessments.
- Address audit findings, implementing changes based on audit recommendations.

Timeline: Audit readiness achieved by Q3 2025.

Responsibility: Sole Proprietor.

Resources:

- Audit software and documentation tools.
- Budget for external audit services.

7.3.2.19. Benefit 19: Strengthened Reputation

Actions:

- Enhance brand messaging by developing marketing materials that highlight security and innovation.
- Engage with customers to foster strong relationships through regular communication.
- Showcase successes by publicizing case studies and client testimonials.
- Monitor brand perception using surveys to track changes in reputation.

Timeline: Reputation advancements by Q3 2025.

Responsibility: Sole Proprietor.

Resources:

- Marketing budget and resources.
- Tools for monitoring brand perception.

7.3.2.20. Benefit 20: Competitive Differentiation

Actions:

- Conduct market research to identify competitive advantages.
- Develop and market unique products and services.
- Engage in thought leadership by publishing articles and participating in industry events.
- Continuously monitor and assess market trends and adjust strategies.

Timeline: Differentiation efforts by Q2 2025.

Responsibility: Project sponsor.

Resources:

- Research and development budget.
- Industry analysis tools.

7.3.2.21. Benefit 21: Visibility and Control

Actions:

- Implement monitoring tools by deploying software for real-time network visibility.
- Enhance control mechanisms by strengthening access controls and security policies.
- Conduct regular reviews to assess and adjust monitoring strategies.
- Train staff in usage of monitoring and control tools.

Timeline: Visibility and control enhancements by Q2 2025.

Responsibility: Project Sponsor.

Resources:

- Monitoring and control software.
- Staff training materials.

7.4. Monitoring and Evaluation

7.4.1. Introduction

The purpose of the Monitoring and Evaluation (M&E) process is to ensure that Project: METAL SNAKE achieves expected benefits by tracking progress and outcomes and adjusting operations as necessary. This process will provide stakeholders with insights into the project's success and inform decision making regarding benefit realization.

7.4.2. Monitoring Plan

7.4.2.1. Metrics and KPIs

The following metrics and key performance indicators will be used to monitor and evaluate the realization of benefits:

- **Cloud cost savings:** Track the monthly server costs against the baseline of $105/month.
- **Security incident reduction:** Count the number of security incidents prevented.
- **Uptime:** Measure the percentage of uptime for both on-premises and cloud hosting.
- **Client satisfaction:** Surveys will be used to gauge customer satisfaction levels.

7.4.2.2. Data Collection Methods

Data will be collected using financial reports, security logs, monitoring tools, and customer feedback surveys.

7.4.2.3. Frequency of Monitoring

Financial metrics and uptime should be tracked monthly. Client satisfaction and security incident metrics should be monitored quarterly.

7.4.3. Evaluation Plan

Evaluation will be conducted annually using criteria such as financial impact, stakeholder satisfaction, and process efficiency. Methods of evaluation will include surveys, data analysis, and interviews to assess project success.

7.4.4. Roles and Responsibilities

The Project Sponsor will oversee the M&E process and be responsible for metrics. Stakeholders will provide input and feedback during evaluations.

7.4.5. Feedback and Continuous Improvement

A feedback loop will be established to gather insights from stakeholders. Continuous improvements will be implemented based on evaluation results.

8. Risk Assessment and Analysis

8.1. Purpose

The purpose of the risk assessment and analysis is to identify potential project risks and formulate strategies to avoid or mitigate their effects, or accept them, or even exploit them.

8.2. Risk Identification

Risk ID	Risk Description	Category
0001	Data loss	Technical
0002	Data protection issues resulting in legal penalties and reputational damage	Compliance
0003	Budget overrun	Financial
0004	Supply chain disruptions	Operational
0005	System failures in hardware and software	Technical
0006	Cost fluctuations (e.g. cloud hosting)	Financial
0007	Human error during installation or configuration	Operational
0008	Failure to comply with regulations	Compliance
0009	Market competition	Strategic
0010	Technological obsolescence	Technical
0011	Exchange rate fluctuations influencing cost	Financial
0012	Resource scarcity of essential equipment	Operational
0013	Insufficient testing	Technical
0014	Cost estimation error resulting in financial discrepancies	Financial
0015	Process inefficiencies resulting in wasted resources or time	Operational
0016	Stakeholder conflict	Strategic
0017	Misalignment with organizational goals	Strategic
0018	Unexpected tax liabilities	Financial
0019	Infringement of intellectual property	Compliance
0020	Global economic conditions affecting financial viability or supply chains	External
0021	Negative reputation of partners	Reputational
0022	Social media backlash	Reputational
0023	Unfulfilled promises or failure to deliver on project	Reputational
0024	Loss of physical premises	Operational
0025	Project Sponsor / Manager dies	Operational
0026	Project requires unanticipated hardware or software	Technical
0027	Difficulty filming in laboratory	Technical
0028	Difficulty completing documentation deliverables on schedule	Operational

8.3. Risk Assessment

Risk #	Risk Description	Likelihood	Impact	Risk Score
0001	Data loss	Possible	Major	Medium
0002	Data protection issues resulting in legal penalties and reputational damage	Possible	Major	Medium
0003	Budget overrun	Possible	Major	Medium
0004	Supply chain disruptions	Possible	Moderate	Medium
0005	System failures in hardware and software	Possible	Moderate	Medium
0006	Cost fluctuations (e.g. cloud hosting)	Likely	Moderate	Medium
0007	Human error during installation or configuration	Likely	Major	High
0008	Failure to comply with regulations	Possible	Critical	High
0009	Market competition	Very likely	Moderate	High
0010	Technological obsolescence	Unlikely	Major	Medium
0011	Exchange rate fluctuations impacting costs	Likely	Moderate	Medium
0012	Resource scarcity of essential equipment	Unlikely	Moderate	Low
0013	Insufficient testing	Possible	Moderate	Medium
0014	Cost estimation errors resulting in financial discrepancies	Possible	Moderate	Medium
0015	Process inefficiencies resulting in wasted resources or time	Likely	Major	High
0016	Stakeholder conflict	Possible	Critical	High
0017	Misalignment with organizational goals	Possible	Major	Medium
0018	Unexpected tax liabilities	Likely	Major	High
0019	Infringement of intellectual property	Unlikely	Major	Medium
0020	Global economic conditions affecting financial viability or supply chains	Possible	Critical	High
0021	Negative reputation of partners	Possible	Moderate	Medium
0022	Social media backlash	Possible	Major	Medium
0023	Unfulfilled promises or failure to deliver on projects	Possible	Major	Medium
0024	Loss of physical premises	Possible	Moderate	Medium
0025	Project Sponsor / Manager dies	Unlikely	Critical	Medium
0026	Project requires unanticipated hardware/software	Possible	Moderate	Medium
0027	Difficult filming in laboratory	Likely	Minor	Medium
0028	Difficulty completing project deliverables on schedule	Likely	Moderate	Medium

Risk Score Matrix

Likelihood / Impact	Minor	Moderate	Major	Critical
Unlikely	Low	Low	Medium	Medium
Possible	Low	Medium	Medium	High
Likely	Medium	Medium	High	High
Very Likely	Medium	High	High	Extreme

8.4. Risk Analysis

Each risk must be analyzed to identify root causes, potential consequences, and interdependencies with other risks.

8.4.1. Analysis of Risk 1

Risk Description: Data loss

Root Causes: Mechanical failure, human error.

Potential Consequences: Loss of digital assets including business administration data and client data.

Interdependencies: Risks #0002, #0005, #0008, #0023

8.4.2. Analysis of Risk 2

Risk Description: Data protection issues resulting in legal penalties and reputational damage.

Root Causes: Cybersecurity incidents, misconfigured software or hardware, human error.

Potential Consequences: Legal penalties and reputational damage.

Interdependencies: Risks #0001, #0005, #0007, #0008, #0011, #0023

8.4.3. Analysis of Risk 3

Risk Description: Budget overrun

Root Causes: Mismanaged project, hardware or software failures required replacement.

Potential Consequences: Project runs out of funding.

Interdependencies: Risks #0006, #0011, #0012, #0014, #0015, #0018, #0020, #0026

8.4.4. Analysis of Risk 4

Risk Description: Supply chain disruptions

Root Causes: Supply scarcity, black swan events (natural disasters, pandemics, etc.)

Potential Consequences: Inability to obtain necessary materials to complete the project.

Interdependencies: Risks #0009, #0011, #0012, #0014, #0016, #0020, #0024, #0026

8.4.5. Analysis of Risk 5

Risk Description: System failures in hardware and software.

Root Causes: Badly configured systems, mechanical failure, buggy software, user error.

Potential Consequences: Need to replace hardware or software, risking budget overrun.

Interdependencies: Risks #0003, #0007, #0010, #0013, #0026

8.4.6. Analysis of Risk 6

Risk Description: Cost fluctuations (e.g. cloud hosting).

Root Causes: Inflation, reliance on a single overpriced vendor for a given solution.

Potential Consequences: Budget overrun, costly cloud hosting fees.

Interdependencies: Risks #0003, #0009, #0011, #0014, #0020

8.4.7. Analysis of Risk 7

Risk Description: Human error during installation or configuration

Root Causes: Improper training, human error.

Potential Consequences: Misconfigured or non-functioning project deliverables.

Interdependencies: Risks #0002, #0005, #0008, #0013, #0023, #0026, #0028

8.4.8. Analysis of Risk 8

Risk Description: Failure to comply with regulations

Root Causes: Human error, ignorance of regulations.

Potential Consequences: Legal liability and costly fines. Damage to reputation and finances.

Interdependencies: Risks #0001, #0002, #0013, #0017, #0018, #0019, #0022, #0023

8.4.9. Analysis of Risk 9

Risk Description: Market competition

Root Causes: Competitors and vendors effect on the market.

Potential Consequences: Low market share compared to competitors, or overly expensive vendor costs.

Interdependencies: Risks #0006, #0010, #0011, #0012, #0020,

8.4.10. Analysis of Risk 10

Risk Description: Technological obsolescence

Root Causes: Continuously improving technology, failure to keep up with technological innovation, depreciation of assets.

Potential Consequences: Poor performance of infrastructure. Loss of market share to better-equipped competitors.

Interdependencies: Risks #0005, #0006, #0009, #0011, #0012, #0023, #0026, #0028

8.4.11. Analysis of Risk 11

Risk Description: Exchange rate fluctuations impacting costs.

Root Causes: Exchange rate fluctuations.

Potential Consequences: Budget overrun, increased cost of operations and goods sold.

Interdependencies: Risks #0003, #0004, #0006, #0009, #0014, #0020

8.4.12. Analysis of Risk 12

Risk Description: Resource scarcity of essential equipment

Root Causes: Shortages of necessary equipment.

Potential Consequences: Disruption in supply chain, schedule overrun waiting for new inventory.

Interdependencies: Risks #0004, $0006, #0009, #0020, #0028

8.4.13. Analysis of Risk 13

Risk Description: Insufficient testing

Root Causes: Human error, ineffective training, failure to comply with good software engineering practices.

Potential Consequences: Misconfigured, faulty, or non-functioning project deliverables. Possible security vulnerabilities.

Interdependencies: #0002, #0005, #0007, #0015, #0023, #0028

8.4.14. Analysis of Risk 14

Risk Description: Cost estimation errors resulting in financial discrepancies

Root Causes: Human error, fluctuating prices, failure to correctly identify costs of the project.

Potential Consequences: Budget overrun, unexpected tax liabilities.

Interdependencies: Risks #0003, #0006, #0009, #0011, #0018, #0020

8.4.15. Analysis of Risk 15

Risk Description: Process inefficiencies resulting in wasted resources or time.

Root Causes: Human error, insufficient training, inefficient business processes.

Potential Consequences: Cost overruns, budget overruns.

Interdependencies: Risks #0003, #0007, #0013, #0014, #0023, #0026, #0028

8.4.16. Analysis of Risk 16

Risk Description: Stakeholder conflicts

Root Causes: Misalignment between project goals and stakeholder expectations.

Potential Consequences: Project failure, loss of premises or necessary equipment for the project..

Interdependencies: Risks #0002, #0003, #0017, #0023, #0024, #0028

8.4.17. Analysis of Risk 17

Risk Description: Misalignment with organizational goals

Root Causes: Poor planning, stakeholder conflicts, scope overrun.

Potential Consequences: Deliverables may not meet project requirements, stakeholder conflicts.

Interdependencies: Risks #0002, #0003, #0016, #0022, #0023, #0028

8.4.18. Analysis of Risk 18

Risk Description: Unexpected tax liabilities.

Root Causes: Misunderstanding of tax law. Poor financial management.

Potential Consequences: Financial penalties, budget overrun.

Interdependencies: Risks #0003, #0008, #0014, #0015

8.4.19. Analysis of Risk 19

Risk Description: Infringement of intellectual property

Root Causes: Human error, misunderstanding of intellectual property laws, insufficient staff training.

Potential Consequences: Legal penalties, including financial penalties.

Interdependencies: Risks #0007, #0008, #0015, #0022

8.4.20. Analysis of Risk 20

Risk Description: Global economic conditions affecting financial viability or supply chains.

Root Causes: Global events and economic conditions.

Potential Consequences: The project could become prohibitively expensive, unprofitable, or supply chains could be disrupted raising costs and delaying project completion.

Interdependencies: Risks #0003, #0004, #0006, #0009, #0011, #0012, #0014, #0023, #0024, #0028

8.4.21. Analysis of Risk 21

Risk Description: Negative reputation of partners

Root Causes: Unethical, unpopular, or illegal behaviour of partners impacting their reputation.

Potential Consequences: Loss of reputation through association. Possible disruption of supply chain or operations if those partners then fail.

Interdependencies: #0004, #0016, #0017, #0022

8.4.22. Analysis of Risk 22

Risk Description: Social media backlash

Root Causes: Dissatisfied customers, cybersecurity incidents and other legal problems, unethical behaviour.

Potential Consequences: Loss of reputation and sales.

Interdependencies: Risks #0001, #0002, #0008, #0017, #0019, #0021, #0023, #0028

8.4.23. Analysis of Risk 23

Risk Description: Unfulfilled promises or failure to deliver on projects

Root Causes: Poor project management, unethical behavior.

Potential Consequences: Reduced customer satisfaction and damage to reputation.

Interdependencies: Risks #0001, #0002, #0003, #0004, #0005, #0007, #0008, #0010, #0012, #0013, #0016, #0025, #0026, #0028

8.4.24. Analysis of Risk 24

Risk Description: Loss of physical premises

Root Causes: Eviction, assignment of new physical premises.

Potential Consequences: Schedule overrun.

Interdependencies: Risks #0016, #0023, #0028

8.4.25. Analysis of Risk 25

Risk Description: Project Sponsor/Manager dies

Root Causes: Accidents or poor health.

Potential Consequences: Project failure.

Interdependencies: Risks #0023, #0028

8.4.26. Analysis of Risk 26

Risk Description: Project requires unanticipated hardware/software

Root Causes: Poor project management, hardware or software incompatibilities or failure.

Potential Consequences: Budget and schedule overruns.

Interdependencies: Risks #0003, #0005, #0010, #0012, #0014, #0015, #0023, #0028

8.4.27. Analysis of Risk 27

Risk Description: Difficulty filming in laboratory

Root Causes: Lack of space, poor management of space, loss or change of premises.

Potential Consequences: Reduced quality of video documentation.

Interdependencies: Risks #0007, #0015, #0016, #0017, #0022, #0023, #0024, #0026, #0028

8.4.28. Analysis of Risk 28

Risk Description: Difficulty completing project deliverables on schedule

Root Causes: Poor project management, insufficient staff training, human error, supply chain issues.

Potential Consequences: Schedule overrun, loss of reputation, dissatisfied customers.

Interdependencies: Risks #0003, #0004, #0005, #0007, #0012, #0013, #0015, #0016, #0020, #0022, #0023, #0024, #0025, #0026

8.5. Risk Mitigation Strategies

[For each risk, outline mitigation strategies, including preventative actions, impact minimization, and responsive actions.]

8.5.1. Strategies for Risk 1:

Risk Description: Data loss

Mitigation: Backup three times to two different media types with one backup stored off-premises.

8.5.2. Strategies for Risk 2:

Risk Description: Data protection issues resulting in legal penalties and reputational damage.

Avoidance: Implementation of firewalls and other preventative measures.

Mitigation: Strong security practices. Implementation of SIEM for security monitoring.

8.5.3. Strategies for Risk 3:

Risk Description: Budget overrun.

Avoidance: Thorough budget planning and costing of required equipment.

Mitigation: Contingency budget.

8.5.4. Strategies for Risk 4:

Risk Description: Supply chain disruptions

Avoidance: Maintain relationships with various vendors.

Mitigation: Buy necessary equipment in advance of implementation.

8.5.5. Strategies for Risk 5:

Risk Description: Systems failure in hardware and software

Avoidance: Good software implementation practices. Thorough documentation.

Mitigation: Contingency budget for replacing hardware and software.

8.5.6. Strategies for Risk 6:

Risk Description: Cost fluctuations (e.g. cloud hosting)

Mitigation: Maintain relationships with different vendors. Train in various cloud platforms.

8.5.7. Strategies for Risk 7:

Risk Description: Human error during installation or configuration

Avoidance: Staff training. Thorough documentation on installation and configuration.

Mitigation: Thorough testing of hardware and software.

Exploitation: Document any repairs or reconfigurations.

8.5.8. Strategies for Risk 8:

Risk Description: Failure to comply with regulations.

Avoidance: Compliance with regulations and regular consultations with a lawyer.

Mitigation: Staff training in regulatory compliance.

8.5.9. Strategies for Risk 9:

Risk Description: Market competition

Mitigation: Maintain competitive prices and excellent customer service. Implement customer feedback systems such as surveys.

Exploitation: Market analysis research to inform improvements on offerings, systems, and technology.

8.5.10. Strategies for Risk 10:

Risk Description: Technological obsolescence

Avoidance: Maintain access to state-of-the-art technology.

Mitigation: Monitor performance of network and websites. Research into new, better technology.

Acceptance: Buy improved technology with the contingency budget.

Exploitation: Identify obsolescence and use it to improve systems with new technology.

8.5.11. Strategies for Risk 11:

Risk Description: Exchange rate fluctuations impacting costs

Mitigation: Contingency budget.

Acceptance: The organization cannot change or affect exchange rate fluctuations.

8.5.12. Strategies for Risk 12:

Risk Description: Resource scarcity of essential equipment

Avoidance: Buy necessary equipment early, before implementation.

Mitigation: Use different vendors to minimize the risks of losing resource availability.

Acceptance: Extend project deadlines to account for delays in equipment delivery.

Exploitation: Buy necessary equipment early and gain advantage over less-equipped competition.

8.5.13. Strategies for Risk 13:

Risk Description: Insufficient testing

Avoidance: Strong and thorough testing practices.

Mitigation: Staff training in testing.

Acceptance: Iteratively fix bugs as they become apparent.

Exploitation: Improve systems while fixing any bugs.

8.5.14. Strategies for Risk 14:

Risk Description: Cost estimation errors resulting in financial discrepancies

Avoidance: Use best practices for cost estimation.

Mitigation: Thorough ongoing research into and monitoring of costs.

Acceptance: Draw on contingency budget.

8.5.15. Strategies for Risk 15:

Risk Description: Process inefficiencies resulting in wasted resources or time.

Mitigation: Continued research into project management and business process efficiency.

Acceptance: Contingency budget.

Exploitation: Document all business processes and attempts to improve process efficiencies.

8.5.16. Strategies for Risk 16:

Risk Description: Stakeholder conflicts.

Mitigation: High level of communication with stakeholders and adherence to their expectations from the project.

8.5.17. Strategies for Risk 17:

Risk Description: Misalignment with organizational goals.

Mitigation: Weekly assessment of project objectives, scope, and alignment with organizational goals.

Acceptance: Realign project with organizational goals.

8.5.18. Strategies for Risk 18:

Risk Description: Unexpected tax liabilities

Avoidance: Store a percentage of profits for tax.

Mitigation: Consult regularly with an accountant.

Exploitation: Document tax liabilities as lessons learned.

8.5.19. Strategies for Risk 19:

Risk Description: Infringement of intellectual property

Avoidance: Awareness of intellectual property law. Avoidance of using copyrighted material.

Mitigation: Regular consultation with a lawyer. Staff training on compliance with intellectual property law.

8.5.20. Strategies for Risk 20:

Risk Description: Global economic conditions affecting financial viability or supply chains

Mitigation: Procure equipment early to avoid disruption in supply chains.

Acceptance: Global economic changes are not within the organization’s control.

Exploitation: Procure equipment early to gain a competitive advantage over less well-equipped competitors.

8.5.21. Strategies for Risk 21:

Risk Description: Negative reputation of partners

Avoidance: Avoid unethical partners or partners with negative reputations.

Mitigation: Maintain relationships with various partners and vendors to provide choice in those the organization deals with.

8.5.22. Strategies for Risk 22:

Risk Description: Social media backlash

Avoidance: Maintain ethical standing and good cybersecurity practices.

Mitigation: Maintain ethical use of social media.

Exploitation: Capitalise on extra publicity.

8.5.23. Strategies for Risk 23:

Risk Description: Unfulfilled promises or failure to deliver on projects

Avoidance: Business process efficiency, process documentation, and extensive project planning practices.

Mitigation: Renegotiate with clients to extend deadlines and, if possible, budgets.

Acceptance: Expend extra organizational resources to fulfill promises and deliver on projects.

8.5.24. Strategies for Risk 24:

Risk Description: Loss of physical premises.

Avoidance: Maintain good relationship with landlords.

Exploitation: Move to better premises, delaying projects but improving facilities and operations.

8.5.25. Strategies for Risk 25:

Risk Description: Project Sponsor/Manager dies

Acceptance: The project and business fail, as there is no-one left to complete the project and execute business operations.

8.5.26. Strategies for Risk 26:

Risk Description: Project requires unanticipated hardware and software.

Mitigation: Thorough project planning, research, and procurement of necessary inventory.

Acceptance: Tap contingency budget to buy the required technology.

8.5.27. Strategies for Risk 27:

Risk Description: Difficulty filming in laboratory

Avoidance: Rearrange laboratory space prior to the execution phase for better shooting opportunities.

Mitigation: Film on other locations when possible.

8.5.28. Strategies for Risk 28:

Risk Description: Difficulty completing project deliverables on schedule.

Avoidance: Add padding time to schedule (one extra week for each phase with heavy documentation requirements).

Mitigation: Work longer hours.

Acceptance: Extend project schedule.

8.6. Monitoring and Review

Risks will be monitored monthly, with regular updates provided to stakeholders. The risk management plan will be reviewed and updated as required.

8.7. Roles and Responsibilities

The following roles and responsibilities have been defined for the project.

Project Sponsor: When the project is complete, all responsibilities will be transferred from the Project Manager to the Project Sponsor.

Project Manager: Will oversee risk management activities, completion of deliverables, and ensure alignment with project goals.

Intern: Will undertake staff training and education in web development, business, and systems administration.

9. Implementation Strategy

This section outlines a comprehensive strategy for executing Project: METAL SNAKE, detailing the steps, resources, and timelines needed to effectively achieve project goals.

9.1. Approach

The approach for implementing Project: METAL SNAKE is based on a phased execution strategy to ensure a systematic and controlled rollout. It includes a combination of waterfall and agile methodologies to balance structured project management with flexibility in construction and development.

9.1.2. Phase 1: Initiation

- Compile documentation necessary to receive stakeholder approval.
- Receive stakeholder approval.

9.1.2. Phase 2: Planning and Design

- Conduct requirements gathering and finalize specifications.
- Develop detailed design and architectural plans.

9.1.3. Phase 3: Execution

- Deploy infrastructure and software solutions.
- Document installation, configuration, and software development.
- Provide training and conduct user acceptance testing.

9.1.4. Phase 4: Testing

- Ensure all systems are thoroughly tested for functionality and integration before deployment.

9.1.5. Phase 5: Deployment

- Final rollout of the completed system.

9.1.6. Phase 6: Maintenance and Closure

- Monitor project performance and outcomes
- Conduct post-implementation review and continuous improvement.

9.2. Timelines

Phase/Subphase	Start Date	End Date	Deliverables
1. Initiation	29/07/2024	11/08/2024	Preliminary Schedule Business Case Stakeholder Register Project Charter Project Manager Assignment Scope Statement Initial Risk Register High-Level Project Plan Introductory Video
2. Planning and Design	12/08/2024	25/08/2024	Project Plan Requirements Document Device Inventory Planning and Design Video
3. Execution: Subphase 1: Server Box	26/08/2024	01/09/2024	Raspberry Pi Server Installation Documentation Raspberry Pi Server Video
3. Execution: Subphase 2: Cloud Server	02/09/2024	08/09/2024	Cloud Server Installation Documentation Google Cloud Server Video
3. Execution: Subphase 3: Firewall	09/09/2024	15/09/2024	Hardware Firewall Installation Documentation Raspberry Pi Firewall Video
3. Execution: Subphase 4: Router	16/09/2024	22/09/2024	Raspberry Pi Router Installation Documentation Rapsberry Pi Router Video
3. Execution: Subphase 5: Wireless Access Point	23/09/2024	29/09/2024	Raspberry Pi WAP Installation Documentation Raspberry Pi WAP
3. Execution: Subphase 6: LAN Installation	30/09/2024	06/10/2024	Physical Cybersecurity Lab Installation Documentation Raspberry Pi LAN Installation Video
3. Execution: Subphase 7: SIEM	07/09/2024	13/10/2024	SIEM Cloud System Installation Documentation SIEM Cloud System Video
3. Execution: Subphase 8: Mautic Email Automation	14/10/2024	20/10/2024	Mautic Email Automation Software Installation Documentation Mautic Email Automation Video
4. Testing	21/10/2024	27/10/2024	Testing deliverables?
5. Deployment	28/10/2024	03/11/2024	Deployment deliverables?
6. Maintenance and Closure	03/11/2024	17/11/2024	Post-Mortem Report Other deliverables?

9.3. Resources

The following resources are required for the completion of Project: METAL SNAKE.

9.3.1. Financial Resources

Budget Allocation for Project: METAL SNAKE (4 Months)					
Category	**Item Description**	**Start Date**	**Est. Cost**	**Frequency**	**Total Cost**
Initial Setup Costs					
Hardware	Computers, network equipment	29/07/2024	$1,485.99	One-Time	$1,485.99
Software	Free open-source software	29/07/2024	$0.00	One-Time	$0.00
Operational Costs					
Internet	Static IP Address	29/07/2024	$10.00	Monthly	$40.00
Hosting	Web server cloud hosting fees		$15.00	Monthly	$45.00
	SIEM cloud hosting fees		$15.00	Monthly	$15.00
Personnel Costs					
Project Manager	Salary	29/07/2024	$0.00	Fortnightly	$0.00
Intern	Salary	29/07/2024	$0.00	Fortnightly	$0.00
Training Costs					
Self-Education	Self-Education	29/07/2024	$0.00	One-Time	$0.00
Training Costs	Intern Training	29/07/2024	$0.00	One-Time	$0.00
Miscellaneous Costs					
Office Supplies	General Office Supplies		$20.00	Monthly	$80.00
Contingency Fund					
Contingency	Reserve for unexpected expenses		$500.00	One-Time	$500.00
				Grand Total	$2,165.99

9.3.2. Human Resources

Project Manager: Will oversee risk management activities, completion of deliverables, and ensure alignment with project goals.

Intern: Will undertake staff training and education in web development, business, and systems administration.

9.3.3. Hardware Resources

The following hardware resources will be required:

- ISP router with Bridge Mode
- Raspberry Pi 5 8GB x 4
- Raspberry Pi 5 Official Case x 2
- Raspberry Pi 5 Unofficial Case x 2
- Raspberry Pi Official Australian Power Adapter x 4
- Raspberry Pi Keyboard
- Raspberry Pi Mouse
- Raspberry Pi Active Cooler x 4
- Micro USB cables x 2
- Network switch
- 512GB SanDisk Extreme Pro MicroSD cards x 4

- 2 x USB 3.0 to LAN Adapters
- 2 x Wireless Network Adapters
- 4-Port USB Hub
- Network Cable x 4

9.4. Tasks and Activities

9.4.1. Phase 1: Initiation

- Create documentation necessary for a high-level overview of the project.
- Obtain stakeholder approval.

9.4.2. Phase 2: Planning and Design

- Gather requirements.
- Develop design documents and architecture plans.
- Review and approve design specifications.

9.4.3. Phase 3: Execution

- Build hardware and application components.
- Ensure proper integration of systems.
- Document all installations, configurations, and software development.

9.4.4. Testing

- Conduct unit, integration, and system testing.
- Address and fix bugs and issues identified during testing.
- Thoroughly document the testing process and results.

9.4.5. Deployment

- Set up IT infrastructure and deploy solutions.
- Conduct training sessions for end-users.
- Perform user acceptance testing and gather feedback.

9.4.6. Maintenance and Closure

- Monitor system performance and user feedback.
- Conduct post-implementation review.
- Finalize documentation, including post-mortem report, user documentation, and technical documentation.
- Implement continuous improvement initiatives.

9.5. Milestones

- **Milestone 1:** Complete project requirements and design specifications (25/08/2024).
- **Milestone 2:** Implement server box and shut down old cloud server instance (01/09/2024).
- **Milestone 3:** Implement cloud server for client website hosting (08/09/2024).
- **Milestone 4:** Finish development and systems testing (27/10/2024).
- **Milestone 5:** Deploy cybersecurity lab and implement user training (03/11/2024).
- **Milestone 6:** Complete documentation, close project, and implement maintenance operations (17/11/2024).

9.6. Dependencies

9.6.1. Technical Dependencies

Availability of development tools and IT infrastructure must be ensured before starting development. The Project Manager should be authorized to deal with the Internet Service Provider Telstra.

9.6.2. Resource Dependencies

Key personnel must be available as scheduled.

9.6.3. External Dependencies

Coordination with vendors and other stakeholders for hardware and software procurement must be completed on schedule.

9.6.4. Stakeholder Dependencies

Timely feedback and approval from stakeholders are required for project phases to progress smoothly.

10. Recommendations

The following details recommendations and justification for the implementation of Project: METAL SNAKE.

10.1. Introduction

The recommendations for Project: METAL SNAKE are based on a comprehensive analysis of project goals, costs, benefits, risks, and strategic alignment with organizational objectives. The recommendations aim to ensure successful implementation and maximize project value and benefits.

10.2. Summary of Key Findings

- The cost-benefit analysis indicates that Project: METAL SNAKE will result in significant cost savings and increased operational efficiencies for the organization.
- The risk assessment identifies critical risks and outlines effective risk management strategies to deal with them.
- The project aligns with the organization's strategic objectives of lowering operational costs and enhancing cybersecurity.

10.3. Specific Recommendations

The following actions are recommended regarding Project: METAL SNAKE:

10.3.1. Proceed with Implementation

- Approve the project for immediate implementation using the phased waterfall method outlined in the Implementation Strategy.
- Ensure all stakeholders are aligned with project objectives and timelines.

10.3.2. Optimize Resource Allocation

- Allocate required financial and human resources as detailed in the Resource Allocation plan to ensure efficient project execution.
- Review resource utilization regularly and adjust allocations as necessary to meet project constraints.

10.3.3. Enhance Cybersecurity Measures

- Prioritize deployment of the cybersecurity lab and SIEM system to manage risks associated with cybersecurity threats and data breaches.
- Allocate resources for continued monitoring and implementation of security protocols.

10.3.4. Focus on Training and Development

- Implement a comprehensive training program to train staff in the skills needed to manage and operate the new technologies efficiently and effortlessly.
- Provide ongoing support and development opportunities to ensure staff competency and information retention.

10.3.5. Monitor and Evaluate Project Outcomes

- Establish a monitoring and evaluation framework to track project progress and measure benefits realization.
- Conduct regular reviews, adjusting strategies based on feedback and performance data.

10.4. Justification for Recommendations

Proceeding with the implementation of Project: METAL SNAKE will deliver a net present value (NVP) of AUD 10,325.42, as outlined in the cost-benefit analysis. This reflects significant financial and operational benefits and the avoidance of costly cybersecurity incidents.

Enhancing cybersecurity measures is critical to protecting sensitive data and maintaining customer trust and organizational reputation, as outlined in the risk assessment.

10.5. Conclusion

By following these recommendations, Project: METAL SNAKE will achieve stated objectives of reducing costs, improving operational efficiency, and enhancing cybersecurity. The project will deliver significant value and also align with organizational goals and strategies, ensuring long-term success and sustainability.

Appendices

Appendix A. Detailed Hardware Specifications

The following hardware will be required to implement the project:

- ISP router with Bridge Mode
- Raspberry Pi 5 8GB x 4
- Raspberry Pi 5 Official Case x 2
- Raspberry Pi 5 Unofficial Case x 2
- Raspberry Pi Official Australian Power Adapter x 4
- Raspberry Pi Keyboard
- Raspberry Pi Mouse
- Raspberry Pi Active Cooler x 4
- Micro USB cables x 2
- Network switch
- 512GB SanDisk Extreme Pro MicroSD cards x 4
- 2 x USB 3.0 to LAN Adapters
- 2 x Wireless Network Adapters
- 4-Port USB Hub
- Network Cable x 4

Appendix B. Project Timeline Chart

Phase/Subphase	Start Date	End Date	Deliverables
1. Initiation	29/07/2024	11/08/2024	Preliminary Schedule Business Case Stakeholder Register Project Charter Project Manager Assignment Scope Statement Initial Risk Register High-Level Project Plan Introductory Video
2. Planning and Design	12/08/2024	25/08/2024	Project Plan Requirements Document Device Inventory Planning and Design Video
3. Execution: Subphase 1: Server Box	26/08/2024	01/09/2024	Raspberry Pi Server Installation Documentation Raspberry Pi Server Video
3. Execution: Subphase 2: Cloud Server	02/09/2024	08/09/2024	Cloud Server Installation Documentation Google Cloud Server Video
3. Execution: Subphase 3: Firewall	09/09/2024	15/09/2024	Hardware Firewall Installation Documentation Raspberry Pi Firewall Video
3. Execution: Subphase 4: Router	16/09/2024	22/09/2024	Raspberry Pi Router Installation Documentation Rapsberry Pi Router Video
3. Execution: Subphase 5: Wireless Access Point	23/09/2024	29/09/2024	Raspberry Pi WAP Installation Documentation Raspberry Pi WAP
3. Execution: Subphase 6: LAN Installation	30/09/2024	06/10/2024	Physical Cybersecurity Lab Installation Documentation Raspberry Pi LAN Installation Video
3. Execution: Subphase 7: SIEM	07/09/2024	13/10/2024	SIEM Cloud System Installation Documentation SIEM Cloud System Video
3. Execution: Subphase 8: Mautic Email Automation	14/10/2024	20/10/2024	Mautic Email Automation Software Installation Documentation Mautic Email Automation Video
4. Testing	21/10/2024	27/10/2024	Testing deliverables?
5. Deployment	28/10/2024	03/11/2024	Deployment deliverables?
6. Maintenance and Closure	03/11/2024	17/11/2024	Post-Mortem Report Other deliverables?