Project: METAL SNAKE

Risk Management Plan

Project Sponsor: Brendan Gasparin

Project Manager: Brendan Gasparin

Date of Project Approval: 14/08/2024

Commencement Date: 29/07/2024

Estimated Completion Date: 24/10/2024

Estimated Project Duration: 17 Weeks

Version: 1.00 (2024-08-24)

1. Executive Summary

1.1. Purpose

The purpose of this Risk Management Plan is to provide a structured approach to identifying, assessing, mitigating, and monitoring risks throughout the lifecycle of Project: METAL SNAKE. The plan aims to proactively address potential risks that could affect the project's success in build an on-premises cybersecurity lab with web hosting capabilities, and integrated cloud services.

1.2. Overview

The overall risk management approach for Project: METAL SNAKE includes regular risk identification sessions, thorough risk assessments using a risk scoring system, and implementing appropriate risk mitigation strategies. Risks will be continuously monitored, and contingency plans will be in place to manage high-priority risks.

Table of Contents

2. Risk Management Approach

2.1. Risk Management Process

The risk management process for Project: METAL SNAKE includes the following steps:

- **Risk Identification:** Risks will be identified at the start of the project and during key project phases. Regular risk identification sessions will be held to ensure that new risks are captured as they arise.
- **Risk Assessment:** Identified risks will be assessed for their likelihood and impact on the project. A risk scoring system will be used to prioritize risks based on their severity.
- **Risk Mitigation:** Mitigation strategies will be developed for high-priority risks, including avoidance, mitigation, transfer, or acceptance. Each risk will be assigned a Risk Owner responsible for implementing the mitigation plan.
- **Risk Monitoring and Control:** Risks will be tracked in a Risk Register, and regular risk reviews will be conducted to monitor the status of risks and adjust mitigation strategies as necessary.

2.2. Risk Identification

Risks will be identified through various methods, including brainstorming sessions within the project team, expert judgment, and consultation with ChatGPT. Identified risks will be documented in the Risk Register and categorized based on their nature (e.g. technical, financial, operational).

2.3. Risk Assessment

Each identified risk will be evaluated based on its likelihood of occurring and its potential impact on the project. Risks will be scored on a scale of 1 to 4 for both likelihood and impact, with the overall risk score calculated by cross-referencing a score for these two values from a risk score matrix. A risk matrix will be used to prioritize risks, with high-priority risks receiving the most attention.

2.4. Risk Mitigation

For each high-priority risk, a specific mitigation strategy will be developed. Strategies may include:

- **Acceptance:** Accepting the risk and its impact on the project.
- **Avoidance:** Modifying the project plan to eliminate the risk.
- **Exploitation:** Turning the risk into a positive opportunity.
- **Mitigation:** Taking actions to reduce the likelihood or impact of the risk.

- **Transfer:** Shifting the risk to a third party, such as through insurance or outsourcing.

2.5. Risk Monitoring and Control

Risks will be continuously monitored throughout the project. The Risk Register will be updated regularly to reflect the status of each risk, and new risks will be assessed as they arise. Risk reviews will be conducted weekly to assess the effectiveness of mitigation strategies and make any necessary adjustments.

3. Roles and Responsibilities

3.1. Project Manager

The Project Manager is responsible for overseeing the risk management process, including facilitating risk identification, assessment, mitigation strategies, and monitoring risk throughout the project. The Project Manager will also track risks and communicate updates to stakeholders.

3.2. Risk Owner(s)

Each risk will be assigned a Risk Owner. Risk Owners are responsible for executing the mitigation strategies and monitoring their assigned risks. They will report any changes in the status of their risks to the Project Manager.

3.3. Project Team

The Project Team will participate in risk identification and mitigation activities. They will report any new risks or changes to existing risks to the Project Manager.

3.4. Stakeholders

Stakeholders will review the Risk Management Plan, approve risk mitigation strategies, and provide input during risk reviews.

4. Risk Identification and Categorization

4.1. Risk Identification Methods

- **Brainstorming Sessions:** Regular brainstorming sessions will be conducted with the Project Team to identify potential risks.
- **Expert Judgment:** Input from subject matter experts will be used to identify risks based on past experience and industry knowledge.
- **Risk Checklists:** Checklists based on lessons learned from previous projects will be used to ensure all potential risks are considered.

4.2. Risk Categories

Risks will be categorized to help prioritize and manage them more effectively. Example categories include:

- **External Risks:** Risks related to external factors such as suppliers, regulatory changes, or market conditions.
- **Financial Risks:** Risks related to budget, funding, and financial management.
- **Operational Rules:** Risks related to day-to-day project operations, resource availability, and logistics.
- **Schedule Risks:** Risks related to project timelines, milestones, and deadlines.
- **Technical Risks:** Risks related to technology, software, hardware, and systems integration.]

5. Risk Analysis

5.1. Risk Scoring System

A risk scoring system will be used to assess the likelihood and impact of each identified risk. Risks will be calculated on a scale of 1-4 for both likelihood and impact. The overall risk score will be calculated by cross-referencing the likelihood and impact scores on a risk score matrix.

5.2. Risk Score Matrix

e.g. A risk matrix will be used to categorize risks based on their scores. The matrix will help prioritize risks by plotting them on a grid with likelihood on one axis and impact on the other. Example categories include:

- **High Priority:** Risks with high likelihood and high impact.
- **Medium Priority:** Risks with moderate likelihood or impact.
- **Low Priority:** Risks with low likelihood and low impact.]

6. Risk Response Planning

6.1. Risk Mitigation Strategies

For each high-priority risk, a specific risk mitigation strategy will be developed. Strategies may include:

Acceptance: Acknowledging the risk and choosing to accept it without taking specific action.

Avoidance: Changing the project plan to eliminate the risk.

Exploitation: Use the risk as an opportunity to improve the project or its performance in some way.

Mitigation: Taking actions to reduce the likelihood or impact of the risk.

Transfer: Shifting the risk to a third party (e.g. insurance or outsourcing).

6.2. Contingency Planning

Contingency plans will be developed for risks that cannot be fully mitigated. These plans will outline the actions that will be taken if the risk occurs.

6.3. Risk Owner(s)

Each risk will be assigned to a Risk Owner who will be responsible for monitoring the risk status and executing the risk response strategy.

7. Risk Monitoring and Control

7.1. Risk Tracking

Risks will be tracked using a Risk Register. The register will include details such as the risk description, category, likelihood, impact, risk score, mitigation strategy, and Risk Owner. The Project Manager will be responsible for updating the Risk Register and sharing it with the Project Team and relevant stakeholders.

7.2. Regular Risk Reviews

Risk reviews will be conducted weekly to assess the status of current risks and identify any new risks. During those reviews, the effectiveness of risk mitigation strategies will be evaluated, and any necessary adjustments will be made. The project manager will lead the risk reviews with input from the Risk Owners.

7.3. Risk Reporting

Risk updates will be included in the regular project status reports. These updates will provide stakeholders with information on the current risk profile, any new risks, and the status of ongoing risk mitigation efforts.

8. Risk Register

ID #	Risk Description	Category	Likelihood	Impact	Risk Score	Risk Owner	Management Strategy	Status	Notes/ Comments
RSK-001	Data loss	Technical	Possible	Major	Medium	PM	**Mitigation:** Backup three times to two different media types with one backup stored off-premises.	Open	
RSK-002	Data protection issues resulting in legal penalties and reputational damage	Compliance	Possible	Major	Medium	PM	**Avoidance:** Implementation of firewalls and other preventative measures. **Mitigation:** Strong security practices. Implementation of SIEM for security monitoring.	Open	
RSK-003	Budget overrun	Financial	Possible	Major	Medium	PM	**Avoidance:** Thorough budget planning and costing of required equipment. **Mitigation:** Contingency fund.	Open	
RSK-004	Supply chain disruptions	Operational	Possible	Moderate	Medium	PM	**Avoidance:** Maintain relationships with various vendors. **Mitigation:** Buy necessary equipment in advance of implementation.	Open	

RSK-005	System failures in hardware and software	Technical	Possible	Moderate	Medium	PM	**Avoidance:** Good software implementation practices. Thorough documentation. **Mitigation:** Contingency budget for replacing hardware and software.	Open	
RSK-006	Cost fluctuations (e.g. cloud hosting)	Financial	Likely	Moderate	Medium	PM	**Mitigation:** Maintain relationships with different vendors. Train in various cloud platforms.	Open	
RSK-007	Human error during installation or configuration	Operational	Likely	Major	High	PM	**Avoidance:** Staff training. Thorough documentation on installation and configuration. **Exploitation:** Document any repairs or reconfigurations. **Mitigation:** Thorough testing of hardware and software.	Open	
RSK-008	Failure to comply with regulations	Compliance	Possible	Critical	High	PM	**Avoidance:** Compliance with regulations and regular consultations with a lawyer. **Mitigation:** Staff training in regulatory compliance.	Open	
RSK-009	Market competition	Strategic	Very Likely	Moderate	High	PM	**Exploitation:** Market analysis research to inform	Open	

							improvements on offerings, systems, and technology. **Mitigation:** Maintain competitive prices and excellent customer service. Implement customer feedback systems such as surveys.		
RSK-010	Technological obsolescence	Technical	Unlikely	Major	Medium	PM	**Acceptance:** Buy improved technology with the contingency budget. **Avoidance:** Maintain access to state-of-the-art technology. **Exploitation:** Identify obsolescence and use it to improve systems with new technology. **Mitigation:** Monitor performance of network and websites. Research into new, better technology.	Open	
RSK-011	Exchange rate fluctuations impacting costs	Financial	Likely	Moderate	Medium	PM	**Acceptance:** The organization cannot change or affect exchange rate fluctuations.	Open	

							Mitigation: Contingency fund.		
RSK-012	Resource scarcity of essential equipment	Operational	Unlikely	Moderate	Low	PM	**Acceptance:** Extend project deadlines to account for delays in equipment delivery. **Avoidance:** Buy necessary equipment early, before implementation. **Exploitation:** Buy necessary equipment early and gain advantage over less-equipped competition. **Mitigation:** Use different vendors to minimize the risks of losing resource availability.	Open	
RSK-013	Insufficient testing	Technical	Possible	Moderate	Medium	PM	**Acceptance:** Iteratively fix bugs as they become apparent. **Avoidance:** Strong and thorough testing practices. **Exploitation:** Improve systems while fixing any bugs. **Mitigation:** Staff training in testing.	Open	

RSK-014	Cost estimation errors resulting in financial discrepancies	Financial	Possible	Moderate	Medium	PM	**Acceptance:** Draw on contingency budget. **Avoidance:** Use best practices for cost estimation. **Mitigation:** Thorough ongoing research into and monitoring of costs.	Open	
RSK-015	Process inefficiencies resulting in wasted resources or time	Operational	Likely	Major	High	PM	**Acceptance:** Contingency budget. **Exploitation:** Document all business processes and attempts to improve process efficiencies. **Mitigation:** Continued research into project management and business process efficiency.	Open	
RSK-016	Stakeholder conflicts	Strategic	Possible	Critical	High	PM	**Mitigation:** High level of communication with stakeholders and adherence to their expectations from the project.	Open	
RSK-017	Misalignment with organizational goals	Strategic	Possible	Major	Medium	PM	**Acceptance:** Realign project with organizational goals. **Mitigation:** Weekly assessment of project	Open	

							objectives, scope, and alignment with organizational goals.		
RSK-018	Unexpected tax liabilities	Financial	Likely	Major	High	PM	**Avoidance:** Store a percentage of profits for tax. **Exploitation:** Document tax liabilities as lessons learned. **Mitigation:** Consult regularly with an accountant.	Open	
RSK-019	Infringement of intellectual property	Compliance	Unlikely	Major	Medium	PM	**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.	Open	
RSK-020	Global economic conditions affecting financial viability or supply chains	External	Possible	Critical	High	PM	**Acceptance:** Global economic changes are not within the organization's control. **Exploitation:** Procure equipment early to gain a competitive advantage over	Open	

							less well-equipped competitors. **Mitigation:** Procure equipment early to avoid disruption in supply chains.		
RSK-021	Negative reputation of partners	External	Possible	Moderate	Medium	PM	**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.	Open	
RSK-022	Social media backlash	Reputational	Possible	Major	Medium	PM	**Avoidance:** Maintain ethical standing and good cybersecurity practices. **Exploitation:** Capitalise on extra publicity. **Mitigation:** Maintain ethical use of social media.	Open	
RSK-023	Unfulfilled promises or failure to deliver on project	Reputational	Possible	Major	Medium	PM	**Acceptance:** Expend extra organizational resources to fulfill promises and deliver on projects. **Avoidance:** Business process efficiency, process	Open	

							documentation, and extensive project planning practices. **Mitigation:** Renegotiate with clients to extend deadlines and, if possible, budgets.		
RSK-024	Loss of physical premises	Operational	Possible	Moderate	Medium	PM	**Avoidance:** Maintain good relationship with landlords. **Exploitation:** Move to better premises, delaying projects but improving facilities and operations.	Open	
RSK-025	Project Sponsor / Manager in poor health	Operational	Unlikely	Critical	Medium	PM	**Acceptance:** The project and business fail, as there is no-one left to complete the project and execute business operations.	Open	
RSK-026	Project requires unanticipated hardware/software	Technical	Possible	Moderate	Medium	PM	**Acceptance:** Tap contingency budget to buy the required technology. **Mitigation:** Thorough project planning, research, and procurement of necessary inventory.	Open	
RSK-027	Difficulty filming in laboratory	Technical	Likely	Minor	Medium	PM	**Avoidance:** Rearrange laboratory space prior to the	Open	

							execution phase for better shooting opportunities. **Mitigation:** Film on other locations when possible.		
RSK-028	Difficulty completing project deliverables on schedule	Operational	Likely	Moderate	Medium	PM	**Acceptance:** Extend project schedule. **Avoidance:** Add padding time to schedule (one extra week for each phase or subphase). **Mitigation:** Work longer hours.	Occurred	Avoidance strategy already implemented.
RSK-029	Miscommunication of information leads to impact on project resources, scope, schedule, budget, or risks	Strategic	Possible	Moderate	Medium	PM	**Mitigation:** A clear communications plan with policies and procedure for communicating with all stakeholders involved with the project.	Open	
RSK-030	Licensing issues with software	External	Possible	Major	Medium	PM	**Mitigation:** Research multiple software solutions for each software component of the project.	Open	
RSK-031	Compatibility problems between software	Technical	Possible	Moderate	Medium	PM	**Mitigation:** Research multiple software solutions for each software component of the project.	Open	

RSK-032	Disruptions in cloud service affect project progress	External	Possible	Major	Medium	PM	**Mitigation:** Maintain awareness and training in various cloud platforms to diversify options.	Open	
RSK-033	Power outages affect project progress	Technical	Possible	Major	Medium	PM	**Mitigation:** Invest in a UPS power supply.	Open	
RSK-034	Network disruptions (e.g. residential Internet outages) affect project progress	Technical	Possible	Major	Medium	PM	**Mitigation:** Obtain authorization to deal with Telstra, to facilitate troubleshooting of external network problems.	Open	
RSK-035	Scope creep introducing new features to the project increasing costs beyond the allocated budget.	Financial	Likely	Moderate	Medium	PM	**Mitigation:** The project scope will be tightly managed to prevent scope creep, with any changes requiring formal approval through the change management plan.	Open	

8.1. Risk Register Key

8.1.1. Examples

Likelihood	Impact	Status
Unlikely (0 – 10%)	Minor	Active (monitoring)
Possible (11-25%)	Moderate	Occurred
Likely (26-50%)	Major	In Progress (resolving)
Very Likely (>50%)	Critical	Closed (resolved)

8.2.2. 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

9. Approval and Sign-Off

The following stakeholders have reviewed and approved the Risk Management Plan for Project: METAL SNAKE:

Project Manager:

Brendan Gasparin X _____

(Signature)

X _____

(Date)

Premises Owner:

[redacted] X _____

(Signature)

X _____

(Date)

Premises Owner:

[redacted]

X _____

(Signature)

X _____

(Date)