**RISK MANAGEMENT PLAN**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | **20th of June, 2023** |
|  |  |  |  | |  |
| Prepared By: | **Shaun Heywood** |  | Project Sponsor: | **OzCazual** | |

|  |
| --- |
| **Strategy** |

The OzCasual cloud infrastructure migration to Amazon AWS is subject to potential risks and vulnerabilities, which are addressed in detail by the Risk Management Strategy for the AWS CyberShift Initiative project. The strategy will cover the key areas of risk identification, assessment, and mitigation.

The key areas of focus for the project are designing safe and secure configurations for Windows and Linux servers, securing the cloud architecture with access controls and encryption, and performing frequent scans and vulnerability assessments. The plan will also pay high attention to the value of log monitoring, real-time network traffic monitoring, red/blue team exercises, technical documentation development, security policy development, and incident response plans. The strategy includes constant risk monitoring, stakeholder communication, and continual improvement through audits and reviews.

In addition to meeting the needs of the business for scalability, the risk management plan will aim to protect the confidentiality, integrity, and availability of systems and customer data. The project can manage risks successfully by putting in place the necessary security controls, performing exercises to find vulnerabilities, and keeping thorough documentation and policies. A comprehensive incident response plan, training and awareness programmes, and regular communication with stakeholders all support the project's risk management efforts.  
  
The strategy places a strong emphasis on maintaining compliance with industry best practices, responding to new risks, and pursuing continuous development. The AWS CyberShift Initiative can successfully safeguard OzCasual's cloud infrastructure and support a secure transfer to Amazon AWS by employing this risk management method.

|  |
| --- |
| **Methodology** |

The risk management plan for the AWS CyberShift Initiative project follows a systematic methodology to identify, assess, mitigate, and monitor risks associated with securing OzCasual's cloud infrastructure and migrating from their existing on premises technology solution, to Amazon AWS. The methodology starts with a thorough risk identification process including stakeholders and SecureNET cybersecurity professionals. Then, a risk assessment is carried out to rank the hazards according to their likelihood and potential consequences. The plan emphasizes the implementation of risk mitigation strategies through the establishment of controls, responsibilities, and timelines.

The methodology will include risk monitoring, communication, and reporting, along with training and awareness programs to promote risk awareness among project team members. Incident response planning, lessons learned, compliance considerations, and documentation will also ensure continuous improvement and adherence to industry best practices.

Overall, this approach offers a defined method for effectively managing risks throughout the project. It helps the project team to engage stakeholders, proactively address vulnerabilities, and keep an open line of communication for risk-related information. This methodology will help the project reduce the negative effects of potential risks, improve project security, and guarantee the AWS CyberShift Initiative is implemented successfully.

|  |  |
| --- | --- |
| **Methodology Step** | **Description** |
| 1. Risk Identification | Engage stakeholders and subject SecureNET experts to identify potential risks and vulnerabilities. |
| 1. Risk Assessment | Assess the identified risks based on likelihood and potential impact. |
| 1. Risk Mitigation | Develop strategies and controls to mitigate the identified risks. |
| 1. Risk Monitoring and Review | Continuously monitor the effectiveness of implemented risk mitigation strategies. |
| 1. Communication and Reporting | Maintain open communication channels and provide regular reports on risk management. |
| 1. Training and Awareness | Conduct training sessions and awareness programs to educate team members on risks and mitigation measures. |
| 1. Incident Response Planning | Develop a robust plan outlining steps to be taken in the event of security incidents. |
| 1. Lessons Learned and Continuous Improvement | Review and learn from past incidents, updating the risk management plan accordingly. |
| 1. Compliance and Audit | Ensure compliance with regulations, standards, and organisational policies. |
| 1. Documentation and Repository | Maintain a central repository for risk-related documentation and knowledge. |

|  |
| --- |
| **Roles and Responsibilities** |

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| **Project Owner** -  Hettige Jayatissa | * Defines the project objectives. * Provide project direction and guidance. * Manage project stakeholders. * Approve project deliverables. * Make decisions and resolve issues. * Manage project constraints. * Ensure project success. * Participate in project governance. * Act as a liaison between the project team and senior management |
| **Project Manager** -  Giuseppe Raciti | * Overall project coordination and management * Plan, organize, and control project activities. * Ensures project deliverables are completed on time and within budget. * Risk management and mitigation * Stakeholder Communication and Reporting |
| **Cyber Security Specialist** -  Shaun Heywood | * Conduct assessments of the existing infrastructure * Design and implement security measures for the cloud infrastructure. * Configure and manage firewalls, IPS/IDS systems, and antivirus/malware protection. * Oversee testing and incident response. * Monitor and analyse logs for potential security threats or breaches. * Provide guidance on security best practices. * Collaborate with the project team to address security vulnerabilities and risks |
| **Cloud Architect / Engineer** -  Mark Byrne | * Designing and configuring the cloud infrastructure on Amazon AWS * Setting up network connectivity with on-site systems * Ensuring scalability and high availability of the cloud environment * Collaborating with the Cyber Security Specialist to implement security measures. * Monitoring and optimizing cloud infrastructure performance * Providing technical expertise on cloud architecture and services |
| **Server Administrator** - Mauricio Guerra | * Collaborating with the project team to ensure a secure transition to AWS. * Assisting in the migration of systems and data to the cloud environment * Configuring and managing the Windows Server 2019 Active Directory server * Supporting the setup and configuration of the Amazon Linux 2 web server * Providing technical assistance during the transition phase * Ensuring the smooth operation of the server infrastructure in the cloud environment |

|  |
| --- |
| **Risk Categories** |

The risk management plan includes various risk categories to ensure comprehensive coverage of potential risks. The categories that the plan covers include infrastructure and cloud security risks, system configuration and software risks, external threats, human factors, compliance, and regulatory risks, as well as project management and stakeholder risks.

The risk management plan considers the above categories to address a wide variety of potential vulnerabilities and risks that might emerge throughout the project. This enables the creation of focused mitigation plans and controls to lessen the effects of risks, assuring the security of the AWS CyberShift Initiative.

|  |  |
| --- | --- |
| **Further details of the categories are:** | |
| **Infrastructure and Cloud Security Risks:** | * Unauthorised access to cloud infrastructure and / or sensitive company data * Inadequate security controls in the cloud environment * Data breaches and / or leakage due to misconfiguration * Service availability issues impacting business operations |
| **System Configuration and Software Risks:** | * Incorrect configuration Windows or Linux servers * Outdated or unpatched software that has known vulnerabilities. * Compatibility issues between different system hardware components * Inadequate security measures for system administration * Inadequate security measures for and user access management |
| **External Threats and Attacks:** | * Malicious threats such as hacking, phishing, or DDoS attacks * Exploitation of vulnerabilities in the network or server infrastructure by malicious threat actors * Social engineering attacks * Compromised third-party services or integrations |
| **Human Factors:** | * Insider threats, including intentional or unintentional. * Lack of awareness * Lack of adherence to security policies * Lack of adherence to procedures * Insufficient training and knowledge about secure best practices * Human error |
| **Compliance and Regulatory Risks:** | * Non-compliance with industry standards and regulations * Non-compliance with legal requirements * Inadequate data privacy protection measures * Failure to meet audit and reporting obligations. * Lack of documentation or evidence of security controls and measures |
| **Project Management and Stakeholder Risks:** | * Insufficient project resources or expertise for effective risk management * Misalignment of stakeholder expectations or priorities * Inadequate communication and collaboration among project team members * Delays or disruptions impacting the project timeline and objectives |

These risk categories encompass a wide range of potential risks that could arise during the AWS CyberShift Initiative's execution. To create effective mitigation measures, it is crucial to further evaluate and rank these risks based on their unique context and effects on the project.

|  |
| --- |
| **Risk Management Funding** |

Risk management funding encompasses the required resources allocated to support the implementation of risk management activities within the AWS CyberShift Initiative Project. The risk management funding would involve the allocation of financial resources for identifying, assessing, mitigating, and monitoring risks associated with securing OzCasual's cloud infrastructure and migrating to Amazon AWS.

Since risk management operations directly impact the project's overall security and success, it is crucial to allot enough budget for them. Organisations can deploy required security measures, maintain an efficient framework for monitoring and responding to risks, and implement effective risk management strategies with the correct funding.

**The funding for risk management would cover the following areas;**

|  |  |
| --- | --- |
| **Risk Assessment Tools and Services:** | The budget would include funds for purchasing or subscribing to tools and services for risk assessment that can be used to find vulnerabilities, run scans, and gauge the likelihood and consequences of potential threats. This would also cover the costs associated for penetration testing services, vulnerability scanning tool licences and providing risk assessments. |
| **Security Controls and Technologies:** | The budget would include funds for purchasing and putting in place the technology, software tools, and security measures necessary to reduce the risks that have been identified. Firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus and malware software, log monitoring and analysis tools, and real-time monitoring solutions may all fall under this category. Budget allocations might also be required for system upgrades or fixes to security flaws. |
| **Training and Awareness Programs:** | The budget would include funds to provide the project team and staff with training sessions and awareness programmes on risk management best practices, secure configurations, and incident response protocols. This would guarantee that the workforce has the knowledge and abilities needed to successfully minimise risks and respond to them. |
| **Incident Response Preparedness:** | The budget would include funds for incident detection, containment, investigation, and remediation as well as to create and maintain an incident response plan. |
| **Risk Monitoring and Compliance Audits:** | The budget would include provisions for continuing risk monitoring operations, such as log analysis, network traffic monitoring, and vulnerability assessments. Funds would also be given for compliance audits to make sure security standards, laws, and policies are followed. |

It is essential to allocate adequate funding to risk management activities as it directly contributes to the overall security and success of the project. Proper funding enables organizations to implement robust risk management strategies, employ necessary security measures, and maintain an effective risk monitoring and response framework.

|  |
| --- |
| **Contingency Protocols** |

Contingency protocols for risk management are predetermined plans and processes that specify how to deal with risks and unforeseen events during the implementation of a project, and how to lessen their effects. Risk management contingency protocols entail adopting strategies and measures to handle identified risks and guarantee business continuity in the face of disruptions or incidents in the AWS CyberShift Initiative.

***Contingency protocols may include the following:***

***Risk Response Strategies:***

Each identified risk will have a corresponding response strategy outlined in the contingency protocols. The strategy could involve risk mitigation, risk transfer through insurance or outsourcing, risk acceptance, or risk avoidance by making alterations to the project plan or scope.

***Incident Response and Escalation:***

In the occurrence of a security incident or risk event, the action to be taken would be specified by contingency protocols. This covers the procedures for incident detection, containment, investigation, and remediation. To ensure that any problems that arise are dealt with in a timely and effective manner, the incident response team will have their roles and duties clearly defined, and escalation procedures will also be specified.

***Backup and Disaster Recovery:***

In case of data loss, system failures, or other serious incidents, contingency protocols will provide backup and disaster recovery strategies. This entails creating frequent backups of crucial data and systems, storing backups off-site, and setting up recovery procedures to resume operations in the event of an incident.

***Communication and Stakeholder Management:***

Guidelines for stakeholder management and communication during risk events or interruptions will be included in contingency plans. This entails designating channels of communication, crucial contacts, and protocols for informing stakeholders about the issue, its effects, and mitigation actions.

***Alternative Solutions and Workarounds:***

If a threat occurs, alternate solutions or workarounds could be considered. Finding backup systems, redundant infrastructure, or contingency plans for short-term business operations may be required.

***Business Continuity Planning:***

Business continuity planning will be addressed by contingency protocols, ensuring that essential business operations can continue in the event of risks and disruptions. This can entail prioritising and maintaining crucial operations by defining procedures, identifying vital individuals, and setting up backup work sites.

Plans for contingencies are essential for reducing risks' effects and assuring the project's resilience. The project team can respond quickly and effectively to unforeseen occurrences, minimise downtime, and protect the integrity and security of the AWS CyberShift Initiative by having established plans and processes in place.

|  |
| --- |
| **Frequency and Timing** |

Risk management frequency and timeliness relates to how frequently risk assessments, mitigation attempts, monitoring, and review processes are carried out to enable successful risk management in the context of the AWS CyberShift Initiative.

The frequency and timing of risk management must be balanced. If risk management activities are conducted too infrequently, hazards may go undetected or mitigation measures may be delayed, while if they are conducted too frequently, resources may be diverted from other crucial project responsibilities.   
  
Based on the particulars of the project, the level of risk exposure, and the requirement for prompt risk identification and response, the best frequency and timing should be chosen.

***Key considerations for risk management frequency and timing are:***

|  |  |
| --- | --- |
| **Risk Assessments:** | To identify potential risks and vulnerabilities related to safeguarding OzCasual's cloud infrastructure and the switch to Amazon AWS, risk assessments should be carried out at the start of the project. To detect any new risks or changes in the risk environment, periodic or milestone-based risk assessments should be carried out throughout the project. |
| **Risk Mitigation:** | Measures for risk mitigation should be put into place as soon as concerns are identified and given a priority. High-priority risks must require immediate mitigation measures, whilst medium- or low-priority risks can wait until a later stage. The urgency and seriousness of the identified threats will determine when to implement risk mitigation measures. |
| **Risk Monitoring and Review:** | Throughout the project, ongoing risk monitoring should be done to identify new risks, changing hazards, or emerging vulnerabilities. Depending on the project, the exposure to risk, and the rate of technical development, different risk monitoring tasks may be conducted more frequently. Regular review sessions should be held to evaluate the efficacy of adopted mitigating measures and make necessary adjustments as required. |
| **Incident Response:** | When a security incident or risk event occurs, incident response procedures should already be set up and prepared to be used right away. To contain the incident and lessen its effects, incident response procedures should be started immediately. To reduce the incident's duration and effects, incident response activities must be coordinated in a time critical manner. |
| **Project Milestones:** | The primary deliverables and project milestones should be coordinated with risk management actions. This guarantees that risk evaluations, mitigation actions, and monitoring are carried out at the proper intervals to support the project's advancement and goals. |
| **Regular Reporting:** | To keep stakeholders updated, regular reporting on risk management actions and the state of identified risks should be scheduled. Depending on the project's timeframe and stakeholder requirements, this can be done on a weekly, monthly, or quarterly basis. |

|  |
| --- |
| **Stakeholder Risk Tolerances** |
| Stakeholder risk tolerances are essential to successful risk management in the AWS CyberShift Initiative project. The degree of risk that each stakeholder is willing to accept or endure inside the project is referred to as stakeholder risk tolerance. Aligning risk management strategies, decision-making procedures, and risk mitigation activities requires an understanding of these risk tolerances.  Different stakeholders may view risk differently; some may be more risk-averse and favour conservative strategies, while others may be more risk-tolerant and willing to accept greater levels of risk. To ensure that risk assessments, mitigation plans, and choices reflect stakeholders' risk tolerances and expectations, effective risk communication and stakeholder engagement are essential.  The risk management plan can be modified to establish a balance between risk reduction and project objectives by taking stakeholder risk tolerances into account. The risk appetites of stakeholders can serve as a guide for risk trade-offs and decision-making processes, ensuring that the chosen risk mitigation techniques match their preferences. |

|  |
| --- |
| **Risk Tracking and Audit** |

The methods and actions involved in recording and evaluating risks over the course of the AWS CyberShift Initiative project are referred to as risk management, risk tracking, and audit. With the help of these procedures, risks should be successfully recognised, evaluated, and managed, and risk reduction measures should be carried out and monitored in a systematic and controlled manner.

***Risk Tracking:***

Risk tracking involves monitoring and recording recognised hazards continuously to evaluate their status and follow changes over time. This involves maintaining an organised database, or risk register, that records and organises risks, their likelihood and impact, existing risk mitigation techniques, and the people or teams in charge.

Potential risks are actively managed by regular revisions to the risk register, which also ensures that alterations or new hazards are quickly discovered. Risk tracking provides project stakeholders with a comprehensive picture of the risk environment, aids in making knowledgeable decisions, and enables prompt adjustments to risk mitigation techniques when necessary.

***Risk Audit:***

The risk audit involves identifying any gaps or potential areas for improvement, evaluating the effectiveness of risk mitigation measures and controls, and determining whether they are being applied as intended. Internal auditors or outside specialists may conduct the risk audit to offer an unbiased evaluation of the project's risk management procedures.   
  
Examining paperwork, conducting interviews, and assessing the risk management framework, policies, and procedures are all typical components of the audit process. The results of the risk audit indicate any new hazards, point out areas where risk management procedures can be strengthened, and offer suggestions for improving risk mitigation strategies.

SecureNET will ensure that risks are regularly tracked, managed, and assessed throughout the AWS CyberShift Initiative project lifecycle by putting in place comprehensive risk monitoring and audit practices. This makes proactive risk management easier, makes it easier for the project to respond to shifting risk scenarios, and gives stakeholders confidence that risks are being effectively managed. Regular risk tracking and audits enable rapid modifications and continual improvement in risk mitigation techniques, which add to the overall efficacy and success of the risk management initiatives.

|  |
| --- |
| **Definition of Probability** |

Risk management probability involves the assessment and estimation of the likelihood that a specific risk event or scenario will occur within the context of the AWS CyberShift Initiative project. The process involves quantifying the probability of various risks occurring based on available data, historical information, judgment, and analysis of relevant factors.

Probability is often rated on a qualitative or quantitative scale during the risk management process. Risks are categorised as high, medium, or low probability based on professional or subjective assessments in qualitative probability assessment. As a result, risks may be prioritised, and the proper resources can be set aside for their mitigation. On the other hand, quantitative probability assessment entails putting numbers or percentages on risks based on statistical analysis, past data, or probabilistic models. This method offers a more accurate and quantitative assessment of the risk's likelihood of happening.

The project team may prioritise their time and resources by determining the likelihood of risks. While risks with lower probabilities can be monitored or managed using less intense procedures, those with higher probabilities may need rapid attention and strong mitigation tactics. The project team can allocate resources effectively, make educated decisions, and create backup plans for hazards that are more likely to materialise thanks to probability assessment. The probability assessment is an ongoing process, and it must be continually examined and revised when new information becomes available, or project conditions change.

|  |
| --- |
| **Definition of Impact by Objective** |

The importance of both qualitative and quantitative factors must be considered when assessing risk effect by objective. To properly prioritise risks, qualitative evaluation involves defining probable impacts as high, medium, or low. In a quantitative assessment, values or scales are assigned to allow for accurate analysis and comparison.

The project team can better allocate resources and establish effective mitigation plans when they are aware of the potential effects of risks. While risks with smaller implications can be addressed with less resources, those with major effects on crucial goals may call for thorough interventions. To ensure alignment with changing project objectives and effectively address new risks, regular review and reassessment of risk implications is a necessary process.

The AWS CyberShift Initiative project can proactively manage and mitigate risks while working to accomplish desired outcomes by considering risk consequences by objective. Decision-making is aided by impact assessment, which enables stakeholders to compare the trade-offs between project goals and risk mitigation initiatives.

***A detailed Risk management impact by objective is as follows:***

***Secure the cloud infrastructure:***

The goal of protecting the cloud infrastructure against security risks may be significantly compromised. Unauthorised access, data breaches, or service interruptions are a few examples of potential dangers. The effects of these risks can include everything from financial losses and lost customer data to reputational harm. To reduce these risks and ensure the security of the cloud infrastructure, effective risk management techniques are required, such as setting up strong firewalls, establishing intrusion detection systems (IPS/IDS), and providing anti-virus/malware protection.

***Installation and configuration of secure Windows 2022 AD Server and Linux Web Server:***

The security and operational efficiency of these servers may be impacted by risks associated with their installation and setup. Vulnerabilities or configuration errors may result in unauthorised access, data loss, or system outages. Compromise of user credentials, system downtime, or unauthorized configuration modifications are only a few examples of the consequences. To mitigate the effects of these risks and preserve the secure operation of the servers, appropriate risk management procedures, such as implementing secure settings, performing vulnerability analyses, and keeping an eye on logs in real-time, are essential.

***Perform external scans/vulnerability assessments:***

Vulnerabilities can be used by malicious actors to obtain unauthorized access, disrupt services, or compromise data if they are not identified and mitigated. The hazards' effects may lead to system breaches, data loss, or service outages. The effect of these risks can be reduced, and the overall security of the infrastructure can be improved, by performing routine scans and producing vulnerability reports with suggested mitigation actions.

***Red/blue team exercises:***

Risks associated with red/blue team exercises centre on locating vulnerabilities and weaknesses in the Linux and Windows Server servers through simulated attacks. These risks have an effect by potentially exposing vulnerabilities in the system and requiring urgent remediation. If flaws identified during the exercise are not fixed, real-world attackers may exploit them and get access without authorisation or compromise the system. The blue team can adopt suitable remediation measures and improve the overall security posture by properly documenting and fixing vulnerabilities discovered during the exercises.

***Handover of technical documentation:***

The potential loss, unauthorised access, or incorrect management of sensitive information contained in the documentation are the key risks connected with the transfer of technical documentation. Impacts can include potential insider threats to compromised security setups and procedures. Secure document handling practices, effective access controls, and the implementation of security policies and procedures should all be part of risk management strategies. The potential impact of these risks can be reduced by adhering to strict risk management procedures during the handover process, protecting the technical documentation's confidentiality and integrity.

The overall goal of risk management impact by objective is to identify, evaluate, and reduce risks that might jeopardise the accomplishment of each individual goal mentioned in the project scenario. SecureNET may reduce the effects of potential risks and improve the overall security, dependability, and integrity of the cloud infrastructure and related systems by putting in place efficient risk management procedures and controls.

|  |
| --- |
| **Probability and Impact Matrix** |

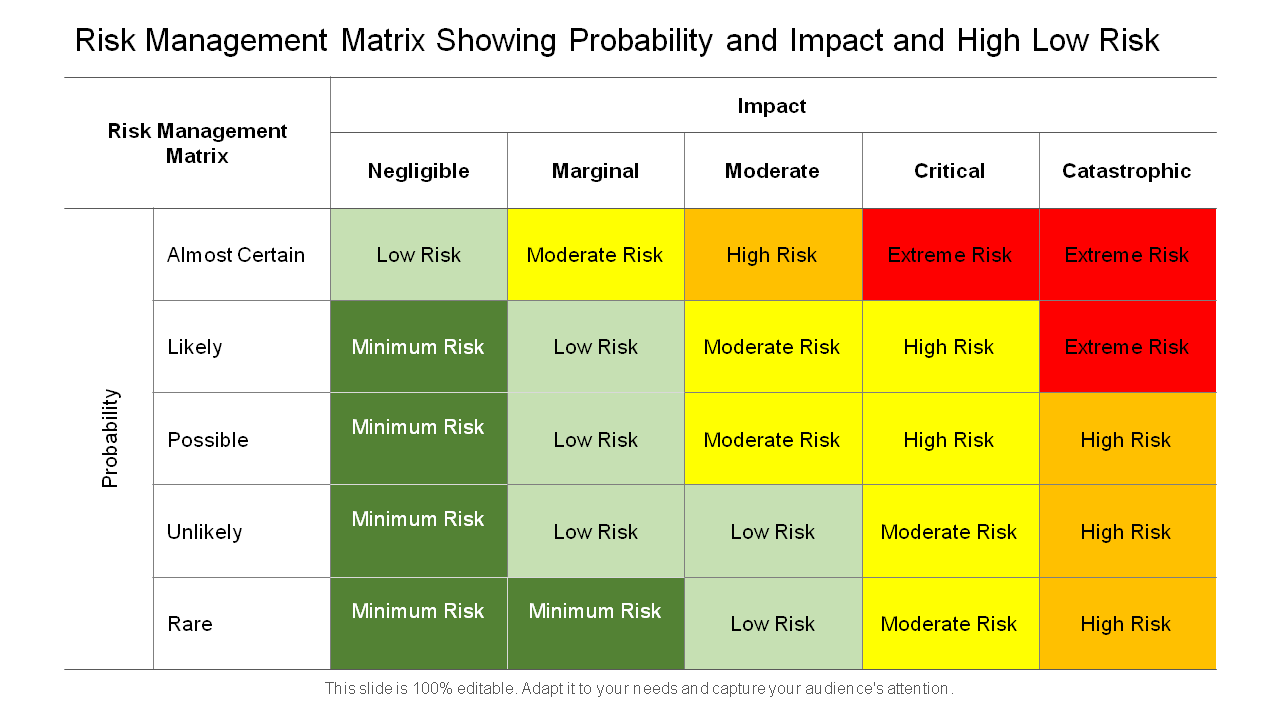
A risk management probability and impact matrix are a tool used to rank hazards according to their likelihood of happening and their influence on the project's goals. A likelihood and impact matrix can assist the project team in the AWS CyberShift Initiative scenario in methodically evaluating and classifying risks for efficient risk management.

The likelihood or chance that a certain risk event will take place is represented by the matrix's probability dimension. It can be evaluated statistically (e.g., percentages) or qualitatively (e.g., low, medium, high) depending on the information at hand, historical data, professional opinion, or mathematical analysis. The probability assessment assists in prioritising risk mitigation activities in accordance with the possibility that dangers may materialise.

The matrix's impact dimension depicts any possible repercussions or effects that the detected risks might have on the project's goals. It evaluates the seriousness and significance of the prospective effects and can be classified statistically (using scales, for example) or qualitatively (using terms like low, medium, and high). Impact analysis improves decision-making processes for risk reduction and resource allocation by assisting in understanding the potential scope of the implications.

The risk management probability and impact matrix enable risks to be divided into various risk levels or zones by combining the probability and impact estimates. This classification aids in prioritising hazards and choosing the best course of action. Risks with high probabilities and high impacts fall into the high-risk zone and require immediate attention and comprehensive mitigation efforts. Risks with low probabilities and low impacts may be deemed acceptable and fall into the low-risk zone, where monitoring or less intensive measures can be applied. The matrix makes it easier to visualise risks, allowing the project team to concentrate on addressing high-priority risks while efficiently allocating resources.

Overall, the AWS CyberShift Initiative project's development of risk mitigation techniques and decision-making processes is supported by the risk management likelihood and impact matrix, which offers a structured method for assessing and prioritising threats. It aids in resource allocation, addresses the most important risks, and makes sure that the risk management activities are in line with the project's priorities and objectives.



**Risk Likelihood table**

|  |  |  |
| --- | --- | --- |
| **Likelihood** | Expected in most circumstances. Has occurred on an annual basis in the past or circumstances are in train that will cause it to happen. | **Almost certain** |
| Has occurred in the last few years or has occurred recently, circumstances have occurred that will cause it to happen in the short term. | **Likely** |
| Has occurred at least once in the history of the organisation or is considered to have a 5% chance of occurring in the current planning cycle or term of the project. | **Possible** |
| Has never occurred in the organisation but has occurred infrequently in other similar organisations or is considered to have around a 1% chance of occurring in the current planning cycle or term of the project. | **Unlikely** |
| Exceptional circumstances only. Is possible but has not occurred to date in any similar organisation and is considered to have very much less than a 1% chance of occurring in the current planning cycle or term of the project. | **Rare** |