Security Risk Assessment &

Treatment Methodology

Classification: **Internal**

This document may only be shared internally without prior confirmation from the owner.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Version** | **Approved**  **By** | **Owner** | **Date Last**  **Updated** | **Review**  **Frequency** | **Next**  **Review** | **Comments** |
|  |  |  |  |  |  |  |

# Purpose of This Document

The following document outlines the overall approach to information security within TechSolution.inc.

It is intended as guidance on crucial aspects of managing critical principles of information security risks.

The content is for staff, auditors, suppliers, and customers. Further supporting details can be found in the referenced policies and procedures.

# The Risk Log

The Information security risk log can be found in the internal file server.

Access to the risk log is restricted to:

* **Information Security Manager:** Full access to view, edit, and manage all entries in the risk log.
* **IT Team:** View access to all risk entries, with edit privileges only for specific entries related to their systems.
* **Senior Management:** View-only access to high-risk items and key decision points.
* **Risk and Compliance Team:** Full access to view and edit risk entries for audit and compliance purposes.
* **External Auditors (as needed):** Temporary view-only access is granted for specific audit periods.

# Roles & Responsibilities

**Information Security Group (ISG)**

* Establishing the organization's risk management policy, objectives, and risk appetite.
* Allocating necessary resources to support the risk treatment process.
* Ensuring risk treatment activities are aligned with the organization's overall strategic objectives.

**Risk owners**

* Identifying and assessing risks associated with their specific areas of responsibility.
* Defining risk criteria and acceptable risk levels.
* Select appropriate risk treatment options (accept, avoid, transfer, or mitigate) based on the organization's risk appetite and criteria.
* Implementing and monitoring risk treatment plans.
* Reporting on risk treatment progress.

**Information Security Officer (ISO):**

* Developing and maintaining the risk treatment methodology and associated tools and techniques.
* Providing guidance and support to risk owners and stakeholders in the risk treatment process.
* Monitoring the overall risk treatment progress and effectiveness. ● Reporting on the risk treatment process to top management and relevant stakeholders.
* Coordinating risk treatment activities.

# Summary of approach

The risk management approach is broken down into five key steps:



# Risk Identification

The identification of security risks can come through many methods. Within the TechSolution.inc, these include, but are not limited to:

* **Annual review of the organization's context** – Any changes to scope, stakeholders, or legislation that may introduce new risks.
* **Monitoring emerging threats** – through alerts from vendors on security threats, updates from the media, and notifications from organizations such as the UK National Cyber Security Centre (NCSC).
* **SWOT analysis** – a method of reviewing an organization's strengths, weaknesses, Opportunities, and Threats. TechSolution.inc undertakes such an assessment of significant threats annually.
* **Stakeholder engagement** – Feedback from staff within and outside the organization.
* **Security audits** – external audits, penetration & vulnerability testing. TechSolution.inc uses both external audits and conducts annual penetration tests.
* **Risk assessment of critical systems** – A top-to-bottom review of components and the likely risks to their continued operation.

Risks should be reported to the Help Desk (if external to IT) and registered in the Risk Log, which will be the single point of truth for the risk details and treatment plan as it progresses through the risk treatment process.

# Risk Assessment

Each risk is then evaluated based on its likelihood and impact. Likelihood refers to the probability of a risk occurring, while impact represents the potential consequences if the risk materializes.

TechSolution.inc has chosen to use the following measurement scales:

|  |  |  |  |
| --- | --- | --- | --- |
| **Likelihood** | | **Description** | **Score** |
| Remote | ●  ●  ● | The risk is improbable to occur under normal circumstances.  There may be no known instances or only a few rare cases in similar organizations or environments.  This category is typically reserved for risks considered negligible or theoretical. | 1 |
| Unlikely | ●  ●  ● | The risk has a low chance of occurring.  It might happen in exceptional circumstances but is not expected to occur regularly.  This level is for recognised risks uncommon in your industry or operational environment. | 2 |
| Possible | ●  ●  ● | The risk has a moderate likelihood of occurring. There is an equal chance of the risk occurring or not occurring.  It's a realistic possibility in your current environment and should be given a fair amount of attention. | 3 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Probable | ●  ●  ● | | The risk is more likely to occur than not. There have been instances of this risk materializing in similar contexts, or there are factors in your environment that increase its likelihood.  It requires proactive management and monitoring. | | 4 |
| Highly Probable | ●  ●  ● | | The risk is almost certain to occur.  Strong evidence or historical data suggests this risk is frequent in your setting.  This level indicates a high-priority risk that demands immediate and effective mitigation measures. | | 5 |
| **Impact** | | **Description** | | | **Score** | |
| Insignificant | | * The impact is negligible, with no notable consequences on operations, reputation, or finances. * It would not cause any interruption to normal business activities or require significant effort to address. | | | 1 | |
| Minor | | * The impact causes a minor inconvenience that can be easily managed or resolved through routine procedures. * It may result in a slight delay or minor costs, but it does not significantly affect business operations or objectives. | | | 2 | |
| Moderate | | * The impact is noticeable and may cause some disruption but can be managed or worked around without significant difficulty. * This level might involve moderate financial costs, a temporary reduction in productivity, or some strain on resources. * It requires management attention but is within the organization's capacity to handle effectively. | | | 3 | |
| Major | | ●  ●  ● | | The impact causes significant disruption to services or operations.  It may result in substantial financial loss, severe damage to reputation, or considerable resource allocation to address.  Recovery from this level of impact requires significant effort and may affect the organization's strategic objectives or long-term plans. | 4 | |
| Catastrophic | | ●  ●  ● | | The impact is so severe that it threatens the existence and continued operation of the organization.  It could lead to long-term or permanent damage to the organization's reputation, financial stability, or market position.  This impact may involve legal ramifications, significant financial losses, and critical damage to organizational assets or stakeholder relationships. | 5 | |

# Risk Prioritisation

TechSolution.inc then ranks the risks based on their likelihood and impact to help focus on the most significant ones. Using a combination of (Impact x Likelihood) gives each risk an overall rating. The top priorities are the high likelihood and high impact quadrant risks.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **IMPACT** | Catastrophic | **5** | 5 | 10 | 15 | 20 | 25 |
| Major Disruption | **4** | 4 | 8 | 12 | 16 | 20 |
|  | Moderate / Workaround | **3** | 3 | 6 | 9 | 12 | 15 |
| Minor / Inconvenience | **2** | 2 | 4 | 6 | 8 | 10 |
| Insignificant | **1** | 1 | 2 | 3 | 4 | 5 |
|  | |  | **1** | **2** | **3** | **4** | **5** |
|  | |  | Remote | Unlikely | Possible | Probable | Highly Probable |
|  |  | **LIKELIHOOD** | |  |

* Red: Extreme risks that threaten the continued operation of the organization.
* Amber: Moderate risks that threaten service operations.
* Yellow: Lower risks that would cause inconvenience but could be worked around.
* Green: Insignificant risks that should be resolved but would cause no notable operational issues.

# Risk Mitigation

The Information Security team will then develop strategies to manage the prioritized risks. There are four main approaches to risk mitigation:

* **Accept**: If a risk has a low likelihood and impact, it might be acceptable to acknowledge and monitor it.
* **Avoid**: If possible, change your plans to avoid the risk altogether.
* **Transfer**: Shift the risk to another party (e.g., through insurance or outsourcing).
* **Mitigate**: Implement actions to reduce the likelihood and/or impact of the risk (e.g., additional training, backup plans, diversifying suppliers).

Risk mitigation plans are then created and monitored, and ownership is assigned for resolving risks to a satisfactory level with which the [Company Name] is comfortable.

The risk log must clearly document the selected risk treatment options (accept, avoid, transfer, mitigate).

Each decision should be justified based on the risk assessment and the organization's risk appetite.

## Documentation

|  |  |
| --- | --- |
| **Accept** | **Provide justification for accepting the risk, including a cost-benefit analysis if applicable.** |
| **Avoid** | Describe the changes made to plans or processes to avoid the risk. |
| **Transfer** | Detail the mechanisms for transferring the risk, such as insurance or outsourcing, and the associated agreements. |
| **Mitigate** | Outline the specific actions taken to reduce the risk, including technical, administrative, and physical controls. |

Risk treatment decisions should be recorded in the risk log, approved by the respective risk owner, and reviewed by the Information Security Officer (ISO).

## Risk Acceptance Criteria

Risk acceptance criteria are defined as the level of risk that the organization is willing to accept without further mitigation.

The criteria are approved by top management based on the organization's risk appetite and strategic objectives.

### Criteria

|  |  |
| --- | --- |
| **Low Risks (Score 1-4):\*\*** | **Acceptable without further treatment, but should be monitored.** |
| **Medium Risks (Score 5-10** | It may be accepted if the cost of mitigation exceeds the benefits. Requires management approval. |
| **High Risks (Score 11-15):\*\*** | Require mitigation measures to reduce risk to an acceptable level. Cannot be accepted without a comprehensive risk treatment plan. |
| **Critical Risks (Score 16-25)** | Unacceptable. Immediate action is required to mitigate or transfer the risk. |

These criteria are reviewed and approved by the Information Security Group (ISG) and are revisited annually or whenever significant changes occur

# Risk Monitoring

Risks are continuously monitored and reviewed, with updates to the risk assessment captured as the situation evolves and the mitigation plans are adjusted accordingly.

Regular risk reviews help ensure that you stay proactive in managing risks and that your approach remains effective.

# Treatment Plans

In our approach to managing and mitigating information security risks, we employ a threshold-based strategy to ensure that each risk is addressed with the appropriate level of detail and attention.

As per our combined likelihood and impact assessment, quantified risks with a score greater than ten warrant the development of a comprehensive risk treatment plan. These plans will provide in-depth strategies and actions tailored to each high-scoring risk's specific nature and complexity, ensuring robust and effective mitigation.

The mitigation strategies and control measures will be documented directly within our risk log for risks that score nine or lower. This approach allows us to maintain a concise and manageable risk log.

while dedicating more detailed planning and resources to risks that pose a more significant threat to our organisation's information security posture.

This methodology aligns with our commitment to a proactive and prioritised risk management process, ensuring that thorough and specific treatment plans address the most significant risks.

The Treatment Plan should be attached to the Risk Record in the Risk Log.

# Escalation

Any risk deemed a 'major' category should be escalated via the management structure to the Corporate Risk Register.