# Risk Management Plan

# Methodology

This **Risk Management Plan** follows the ISO 27001 and GDPR-compliant framework to assess and mitigate potential risks to the information security and data privacy of Waquis (Pvt) Ltd. The risk assessment process begins with a structured **risk identification** phase, where all potential risks to the company’s IT infrastructure, data management processes, and compliance requirements are identified.

Key risks include data breaches, non-compliance with regulatory standards, and operational disruptions. After identifying these risks, they are evaluated through a **risk analysis** process, where the likelihood of each risk occurring and its potential impact on the organization are determined. This analysis uses both **qualitative** and **quantitative** techniques, in line with ISO 27001 guidelines, to ensure a deep understanding of how these risks could affect business continuity, legal compliance, and the company's reputation.

The next step is **risk evaluation**, where identified risks are ranked by their severity. This is particularly critical for risks involving data breaches or regulatory non-compliance. The final stage, **risk treatment**, focuses on implementing risk mitigation strategies outlined in ISO 27001 while ensuring data protection measures that meet GDPR obligations. Continuous monitoring and evaluation are essential to ensure that the risk management plan remains adaptable to emerging threats, protecting the organization’s security and compliance.

# Risk Identification

In this phase, we systematically identify all potential threats and vulnerabilities that could compromise the company’s information security and personal data. This involves creating a comprehensive **asset inventory**, mapping **data flows**, and reviewing **existing processes** for weaknesses. The following risks were identified through this process:

* **Unauthorized access to sensitive customer data**.
* **Data breaches caused by external cyberattacks**.
* **Insider threats from malicious employees**.
* **Malware infections due to weak endpoint security**.
* **Physical theft of devices holding important data**.
* **Non-compliance with data privacy laws**.
* **Denial-of-Service (DoS) attacks disrupting essential services**.

By thoroughly analyzing these risks, we lay the foundation for an in-depth and effective risk assessment.

# Risk Analysis

Each identified risk is analyzed based on its **potential impact** and **likelihood** of occurrence using a **risk matrix**. The matrix helps prioritize risks based on their severity to the organization:

| **Risk** | **Likelihood** | **Impact** | **Current Controls** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Unauthorized access to sensitive data | High | Severe | Password protection, multi-factor authentication | Critical |
| Data breach from external cyberattacks | Medium | Severe | Firewalls, Intrusion Detection Systems | High |
| Insider threats | Low | Moderate | Employee monitoring, access control lists | Medium |
| Malware infections | Medium | High | Antivirus software, regular software updates | High |
| Physical theft of devices | Low | High | Regular compliance audits, policy enforcement | Medium |
| Denial-of-Service attacks | Medium | Moderate | Distributed Denial-of-Service (DDoS) protection | Medium |

This analysis provides a detailed understanding of each risk’s potential effect on business continuity, compliance, and security, and helps prioritize risks for further treatment.

# Risk Calculation

After identifying and analyzing the risks, the next step is to calculate the **overall risk level**. The risk calculation formula combines the **likelihood** of the risk with its **potential impact** to produce an overall risk score. This score helps determine which risks require immediate action.

# Risk Evaluation

During the risk evaluation phase, we assess the likelihood and severity of each identified risk. We prioritize risks based on their potential impact on data security and the company's ability to remain compliant with GDPR and ISO 27001 regulations.

The following risks have been ranked according to their criticality:

* **Unauthorized access to sensitive data**: **Critical**
* **Data breach from external cyberattacks**: **High**
* **Malware infections**: **High**
* **Physical theft of devices**: **Medium**
* **Denial-of-Service attacks**: **Medium**

By evaluating and ranking these risks, we can determine which risks require immediate attention and which can be managed through ongoing monitoring and mitigation measures.

# Risk Treatment

Following the evaluation, the appropriate risk treatment strategies are developed based on ISO 27001 standards. Treatment options include:

* **Mitigation**: Implementing additional security controls, such as stronger encryption, stricter access controls, and improved incident response procedures.
* **Avoidance**: Altering business processes to remove the risk entirely, such as discontinuing the use of systems with known vulnerabilities.
* **Transfer**: Outsourcing certain functions to third-party vendors or obtaining cybersecurity insurance to transfer the risk.
* **Acceptance**: In cases where the cost of mitigation outweighs the potential impact, the organization may decide to accept the risk but continue monitoring.

For each risk, a specific action plan is developed, including timelines, responsible personnel, and the required resources.

**7. Ongoing Monitoring and Review**

Once the risk management strategies are in place, ongoing monitoring and review are essential to ensure the organization remains protected. Regular audits, vulnerability assessments, and compliance checks help maintain the integrity of the risk management plan. Additionally, the organization must stay vigilant to emerging threats and continually update its risk management practices.

The risk management process should be revisited regularly to ensure that all controls remain effective, and that the organization adapts to new and evolving risks.