Foodie Information Risk Treatment Plan

# 

# 

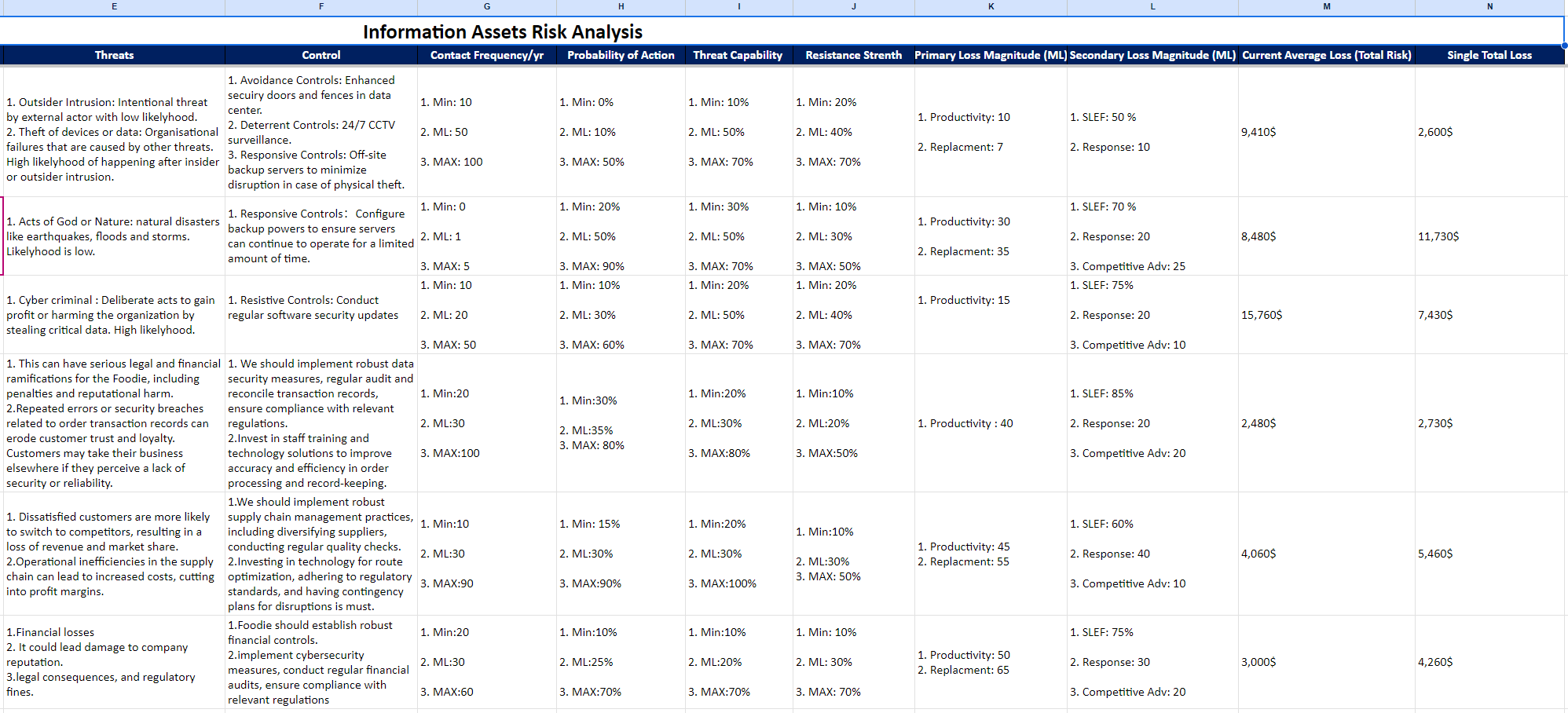
# Purpose:

Foodie’S Information Risk Treatment Plan is a comprehensive strategy for mitigating information security risks within the context of the food industry. It's a crucial component of a broader information security program that helps protect sensitive data and ensure the integrity, confidentiality, and availability of information.

# Risk Treatment Decision Process

In Foodie, we have conducted proper risk evaluation in the TRA table to help us in the risk treatment decision process. It helps Foodie to understand the potential losses that might incur if a specific risk scenario realsies. Full risk loss calculation can be found in the document “Foodie ISMS tables”.

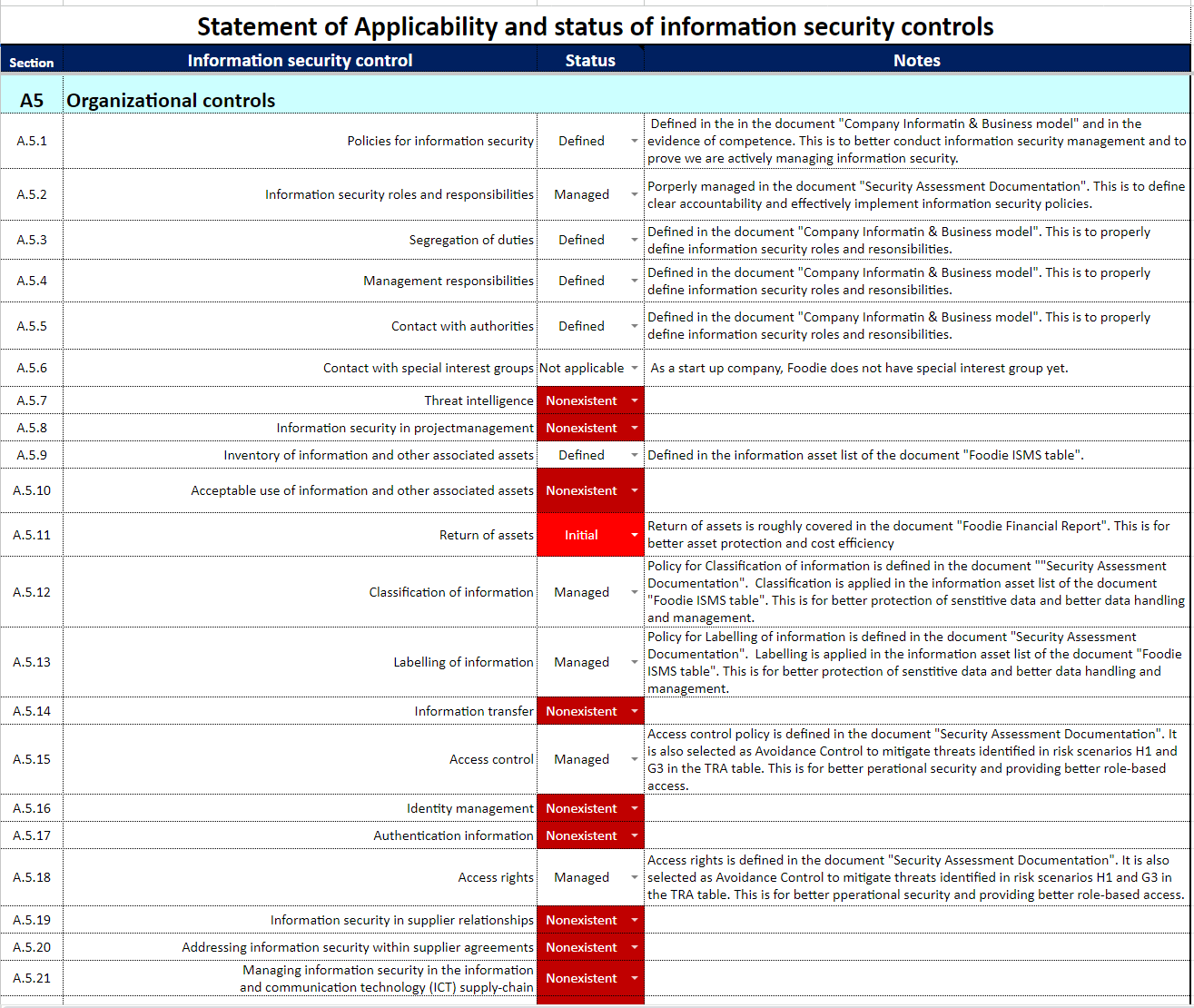
* Prioritization of Risks: By quantifying potential losses, Foodie can prioritize risks in order of magnitude, ensuring that the most severe threats are addressed first and its controls are selected accordingly.
  + Use of OpenFair Risk Analytic tool.
* Cost efficiency analysis: With clear loss calculations, Foodie can allocate appropriate resources for mitigation strategies and ensure that they are financially prepared for potential risks.
  + Current Average loss (total risk): It describes the average financial loss per year of a specific risk scenario of one of Foodie’s critical assets.
  + Single total loss: It describes the potential financial loss of a specific risk scenario of one of Foodie’s critical assets that happens once.
  + Contact Frequency: the frequency with which a threat event (e.g., a cyber attack) comes into contact with Foodie’s vulnerable asset or system.
  + Primary Loss Magnitude: Once a threat event occurs, PLM determines the magnitude of loss that results directly from that event. In Foodie’s context, it is a loss of productivity for our delivery service.



*Risk Evaluation with OpenFair Risk Analytic tool*

The statement of applicability has also been identified to help Foodie ensure that all potential risk treatments (controls) are considered, justified, and documented. Foodie’s SOA document outlines which of the standard’s controls are applicable to Foodie and explains why those controls have been selected. Full document can be found in “Foodie The Statement of Applicability”

* Clarifying Relevant Controls: The SOA provides a comprehensive list of controls and their applicability. Foodie can quickly identify which controls are relevant to which risks, streamlining the treatment decision process.
* Gap Analysis: The SOA helps identify areas where current security measures may be lacking, aiding the decision-making process on what additional controls are needed.
* Explaining Control Choices: The explanations in the SOA provide a rationale for why certain controls were chosen and others were excluded. This reasoning can guide risk treatment decisions by providing context and clarity.
* Continuous Improvement: As risks evolve, Foodie will continuously update the SOA document, ensuring that the risk treatment decision process is always based on current, relevant information.



*Foodie’s SOA*

# 

# 

# 

# 

# 

# 

# Risk Treatment Options Selection

**How the controls are selected:**

Given the information found in the loss calculations, a systematic approach that considers various risk parameters is essential. We will mainly use the following four risk parameters when selecting the appropriate controls:

* Current Average Loss (Total Risk): This value essentially offers a historical perspective on the financial implications of a specific risk scenario. Controls for risks that historically have a higher average loss would likely be prioritized. In essence, by focusing on controls that address these high average loss scenarios, Foodie can potentially achieve a significant reduction in its overall risk posture.
* Single Total Loss: This is about assessing the maximum potential damage of a risk scenario. Even if a particular threat has a low frequency, if its potential damage (or single total loss) is extremely high, it might still warrant significant attention.
* Contact Frequency: Controls selected based on contact frequency would primarily focus on the most frequently occurring threats. A high contact frequency indicates a regular or recurring threat, and measures should be in place to either prevent these occurrences or mitigate their effects when they occur.
* Primary Loss Magnitude (Productivity Loss for Delivery Service): This metric focuses on the operational impact of a threat event. If a threat leads to a significant loss of productivity, even if its direct financial impact is low, it's crucial to address it. The rationale here is that disruptions to Foodie’s core services (like delivery) could lead to long-term reputational damage, customer attrition, and other indirect costs.

**WWMD and Consequence Table:**

By gathering the information of the four major parameters, we can use the information to determine and finalize the criticality of risks and how we should handle such risks by using WWMD, consequence table and the defined risk appetite.

**Risk Retention**

According to the WWMD table, if the Single Total Loss of one particular risk is less than 5,000$ or the primary loss magnitude (percentage of delivery service affected) is less than 25%, we consider this risk level medium and it is tolerable. Foodie will accept the residual risks.

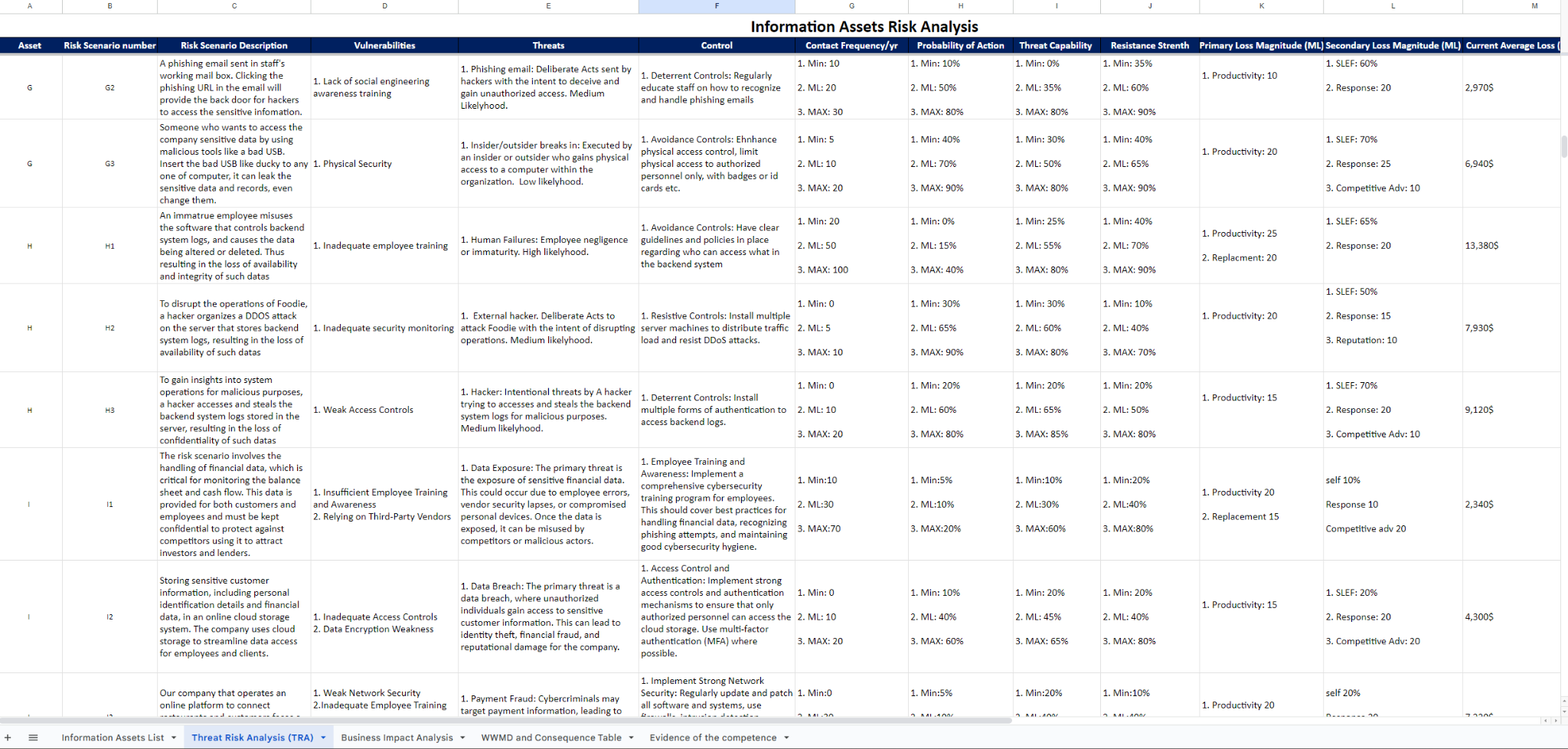
**Risk reduction**

If the Single Total Loss of one particular risk is more than 5,000$ or the primary loss magnitude (percentage of delivery service affected) is more than 50%, we consider this risk level is high and it is intolerable. Appropriate controls will be implemented to mitigate such risk.

**Based on the information produced from the risk treatment decision process, the following are some of the examples of the risk controls we have identified:**

* Risk scenario A1: An outsider breaks in the main data center and steal the critical server hardware to disrupt the operations of Foodie
  + Current Average Loss (Total Risk): 9,410$
  + Single Total Loss: 2,600$
  + Contact Frequency: Most likely 50/yr
  + Primary Loss Magnitude: 10
    - Avoidance Controls: Enhanced security doors and fences in the data center.
* Risk scenario A2: Natural disasters damage the power supply in the main data center, resulting in the dysfunction of servers
  + Current Average Loss (Total Risk): 8,480$
  + Single Total Loss: 11,730$
  + Contact Frequency: Most likely 1/yr
  + Primary Loss Magnitude: 30
    - Responsive Controls：Configure backup powers to ensure servers can continue to operate for a limited amount of time.
* Risk scenario A3: A cyber criminal hacks the servers in the main data center and gains unauthorized access to sell critical data of Foodie
  + Current Average Loss (Total Risk): 15,760$
  + Single Total Loss: 7,430$
  + Contact Frequency: Most likely 20/yr
  + Primary Loss Magnitude: 15
    - Resistive Controls: Conduct regular software security updates
* Risk scenario B1 :Access to order transaction records without authorization can result in a data breach. This can lead to the theft of important client information such as credit card numbers, addresses, and phone numbers.
  + Current Average Loss (Total Risk): 2,480$
  + Single Total Loss: 2,730$
  + Contact Frequency: Most likely 30/yr
  + Primary Loss Magnitude: 40
    - We should implement robust data security measures, regular audit and reconcile transaction records, and ensure compliance with relevant regulations. 2.Invest in staff training and technology solutions to improve accuracy and efficiency in order processing and record-keeping.
* Risk scenario B2 :Disruptions in the supply chain (e.g., ingredient shortages, transportation issues) can affect food availability and delivery times.
  + Current Average Loss (Total Risk): 4,060$
  + Single Total Loss: 5,460$
  + Contact Frequency: Most likely 30/yr
  + Primary Loss Magnitude: 45
    - We should implement robust supply chain management practices, including diversifying suppliers, conducting regular quality checks. 2.Investing in technology for route optimization, adhering to regulatory standards, and having contingency plans for disruptions is a must.
* Risk scenario B3 :Unauthorized or fraudulent financial transactions, including embezzlement or internal fraud by employees.
  + Current Average Loss (Total Risk): 3,000$
  + Single Total Loss: 4,260$
  + Contact Frequency: Most likely 30/yr
  + Primary Loss Magnitude: 50/yr
    - Foodie should establish robust financial controls. 2.implement cybersecurity measures, conduct regular financial audits, ensure compliance with relevant regulations
* Risk scenario G1 :Malware like viruses,worms, and ransomware could disrupt all the laptops or PCs to gather sensitive information.
  + Current Average Loss (Total Risk): 5,710$
  + Single Total Loss: 960$
  + Contact Frequency: Most likely 35/yr
  + Primary Loss Magnitude: 10
    - Deterrent Controls: Install and keep antivirus software up-to-date on operating systems
* Risk scenario G2 :A phishing email sent in the staff's working mailbox. Clicking the phishing URL in the email will provide the back door for hackers to access the sensitive information.
  + Current Average Loss (Total Risk): 2,970$
  + Single Total Loss: 480$
  + Contact Frequency: Most likely 20/yr
  + Primary Loss Magnitude: 10
    - Deterrent Controls: Regularly educate staff on how to recognize and handle phishing emails
* Risk scenario G3 :Someone who wants to access the company's sensitive data by using malicious tools like a bad USB. Insert the bad USB like ducky to any computer, it can leak the sensitive data and records, even change them.
  + Current Average Loss (Total Risk): 6,940$
  + Single Total Loss: 3,220$
  + Contact Frequency: Most likely 10/yr
  + Primary Loss Magnitude: 20
    - Avoidance Controls: Enhance physical access control, limit physical access to authorized personnel only, with badges or id cards etc.

**Full list of identified controls can be found in the TRA table in the document “ Foodie ISMS TAbles”.**

****

*List of identified controls*

**Residual risks:**

Foodie need to deal with residual risks, especially those deemed unacceptable after the application of controls. We seek to ensure that all activities undertaken by Foodie are within acceptable risk parameters, aligning with our commitment to safeguarding our stakeholders and assets.

* Re-evaluation of Current Controls: All current risk controls shall be regularly reviewed for their efficacy. If they are found wanting, enhancement or fortification measures should be considered. Where necessary, redundant controls will be introduced to ensure risk is managed to acceptable levels.
* Risk Avoidance: Activities or processes that consistently yield unacceptable risks, after comprehensive analysis, may be recommended for discontinuation or replacement.
* Risk Transfer: Financial tools such as insurance will be considered to mitigate potential financial losses arising from realized risks. Functions that are deemed too risky and better managed externally may be outsourced to specialists.

# Ongoing Monitoring and Review

| Entry # | Date & Time | Updated by | Reasons for update | Change description |
| --- | --- | --- | --- | --- |
| 1 | 21/10/2023 | CIO: Guangye Li | To have an better risk treatment plan document that meet the requirements of Foodie’s internal audits | Redesigned risk treatment plan document |
| 2 | 23/10/2023 | CIO: Guangye Li | To have clear procedures for residual risks that are unacceptable | Add policy and procedures for residual risks |
|  |  |  |  |  |
|  |  |  |  |  |