Foodie: Information Security Risk Assessment Process Documentation

In accordance with ISO 27001, ISO 27005

# Purpose

The purpose of this document is to outline Foodie's process for conducting Information Security Risk Assessments in accordance with ISO27001, ISO 27005. The process aims to be structured, repeatable, and adaptable to changes in the information risk environment specifically tailored to the food and restaurant industry.

# Scope

This document covers all the risk assessment process that related to Foodie’s business processes and information assets, including risk identification, analyzation, evaluation, and prioritization. It will be constantly reviewed and updated to reflect the changes in our approaches to risk assessment. This documentation will also briefly cover the major conflicts and decision-making behind the management team’s efforts to conduct risk assessment as a reference.

# Risk Identification

To properly detect and document the risks that could potentially have a negative impact on Foodie. The following actions have been implemented.

* Identification of major information assets
* Identification of the risk scenarios of the major information assets
* Assignment of information assets’ owner
* Identification of information assets’ classification and labelling

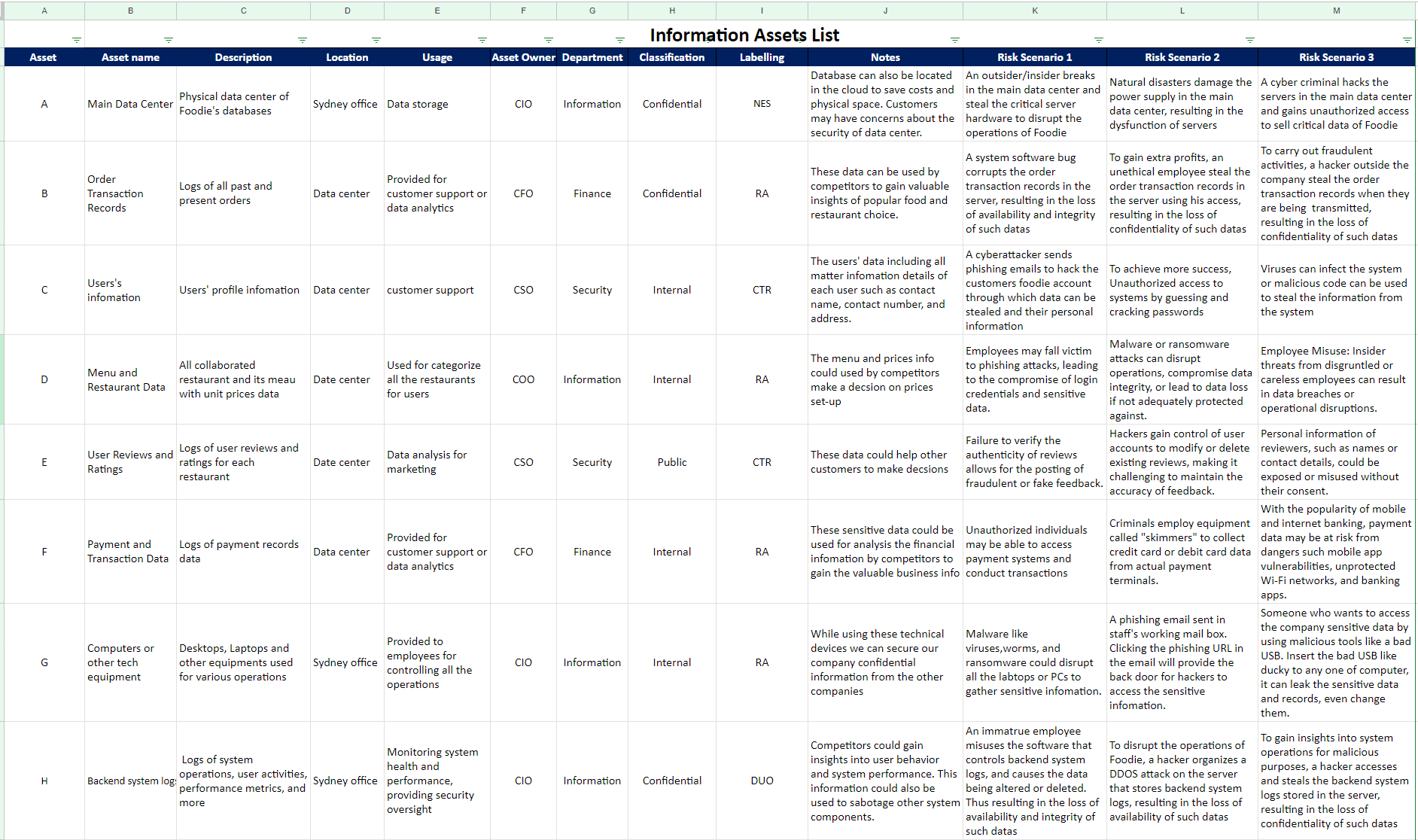
Figure 1.a shows a fraction of Foodie’s information assets list. The information assets list has been updated and improved with information assets’ classification and labelling according to Foodie’s new information classification policy. Figure 1.b shows the updated information assets list. The policy can be found in the document “Security Assessment Documentation.”

To view the full list, please visit the file “Foodie’s ISMS table”.

A screenshot of a computer

Description automatically generated

*Figure 1.a. Old Information Assets List*



*Figure 1.b. New Information Assets List*

## Major conflicts and decision-making

During the first phase of risk identification, the management team engaged in a debate regarding the issue of the ownership of information assets, particularly between CIO and CTO. The debate was mainly due to the insufficient knowledge and experience of the management team. After conducting in-depth research and learning throughout multiple weeks, a mutual agreement is finally settled. After that, the risk identification process is smooth. The team is still concerned the information assets list doesn’t cover all the major aspects of Foodie’s business process. Hence the list will potentially be updated in the coming weeks.

After week 09, one major change is the addition of information classification and labelling. To better classify and label our critical information assets, the group decided to write information classification policy document as a guide. A screenshot of a chat

Description automatically generated

# Risk Analyzation

To assess potential threats and vulnerabilities of the valuable information assets of Foodie accurately and systematically, the following processes have been implemented.

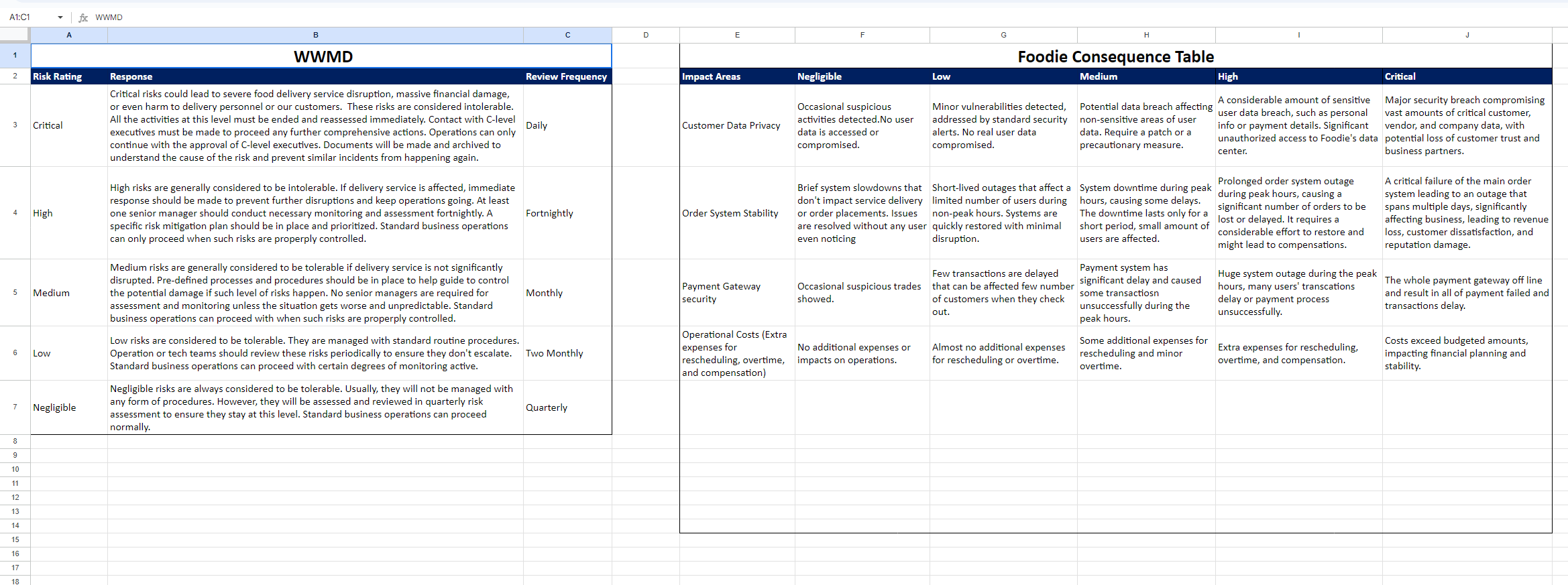
* Risk scenarios analysis (TRA): To systematically identify and evaluate Foodie’s critical information assets’ potential threats and associated vulnerabilities that could negatively impact the Foodie's operations and business objectives.
* WWMD Table: The WWMD table provides a structured approach for management's response to various risk scenarios. It offers a roadmap on the actions to be taken based on the magnitude or severity of a particular risk.
* Consequence Table: The consequence table categorizes risks based on their potential impact. It helps in understanding the severity of a risk event and thus guides Foodie’s risk treatment decisions.
* Business Impact Analysis: Business Impact Analysis is to systematically evaluate and quantify the potential effects of interruptions or disruptions to Foodie’s food delivery service.

Figure 2.a illustrates WWMD and Consequence table before Week 8. After receiving comments from internal audits, quantitative information is integrated into the WWMD and Consequence table. Figure 2.b illustrates WWMD and Consequence table after updates.

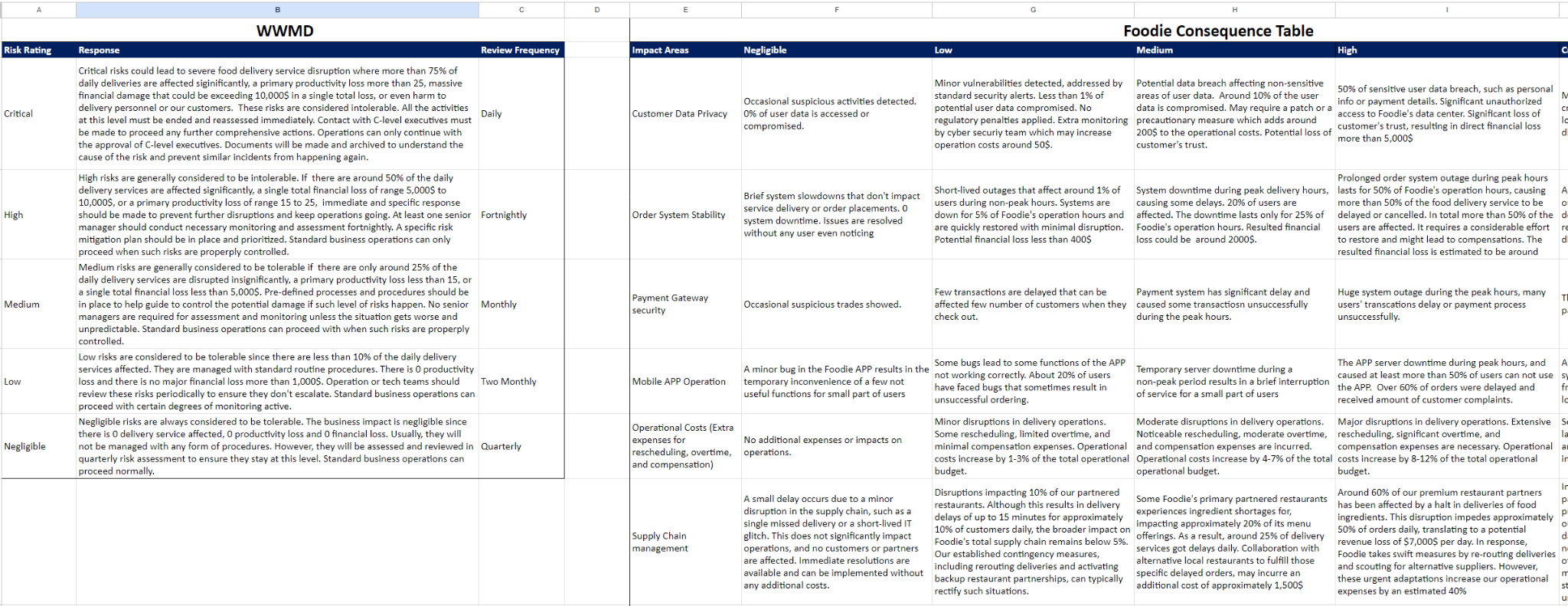
In week 07, the management redesigned risk scenario analysis as we gained a better understanding of threats and controls. Figure 3.a illustrates the re-designed threat risk analysis table separated from figure 1. After Week 08, the management improved TRA using a more sophisticated method of loss calculation: OpenFair risk analytic tool. Figure 3.b illustrates the improved TRA table integrated with OpenFair risk analytic tool.

In week 09, to properly evaluate the potential impact of the critical information assets on the business continuity of Foodie. BIA is conducted and integrated with TRA table. Figure 3.c shows the TRA table integrated with BIA.

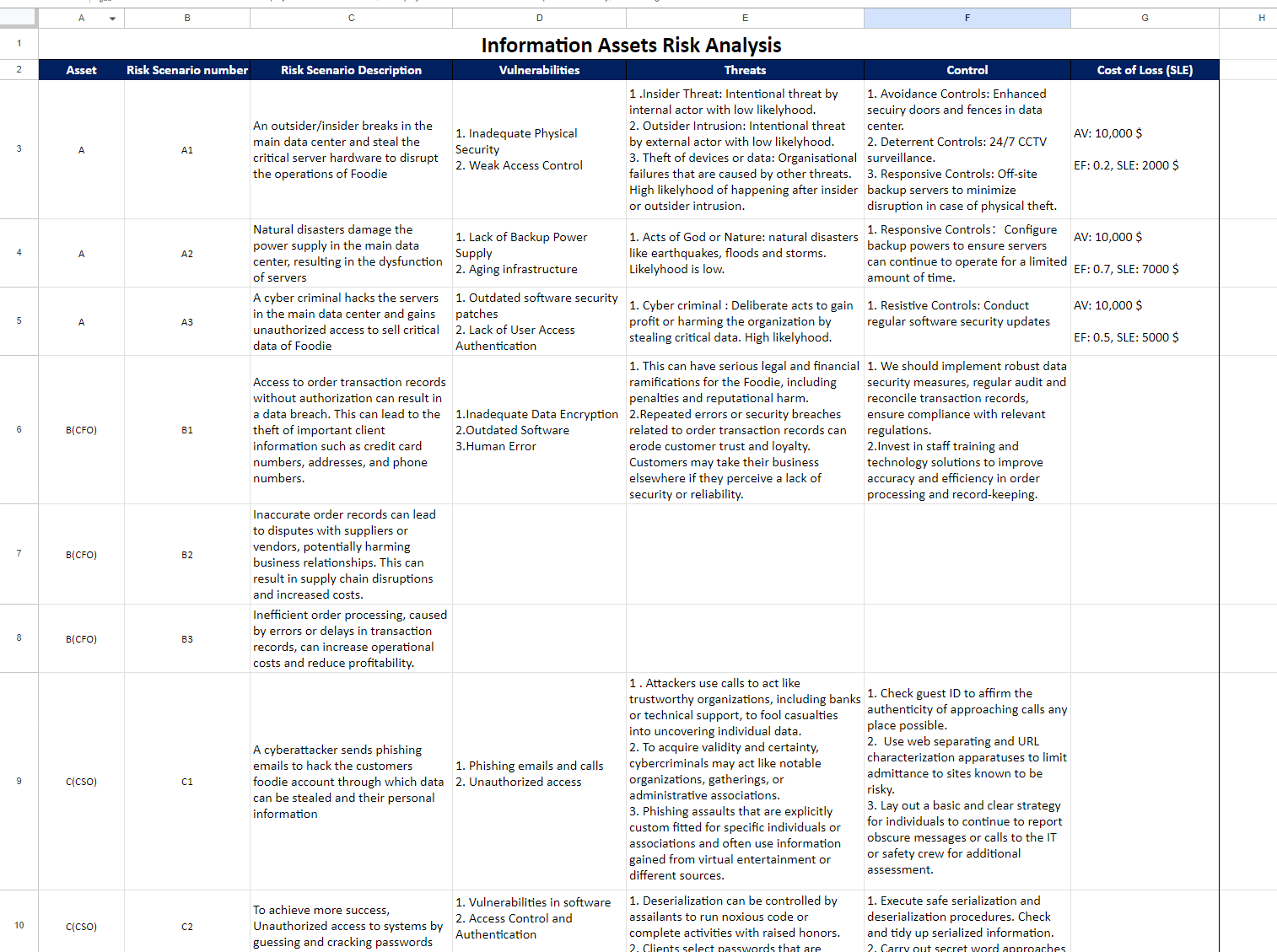
To view the full tables, please visit the file “Foodie ISMS table”.



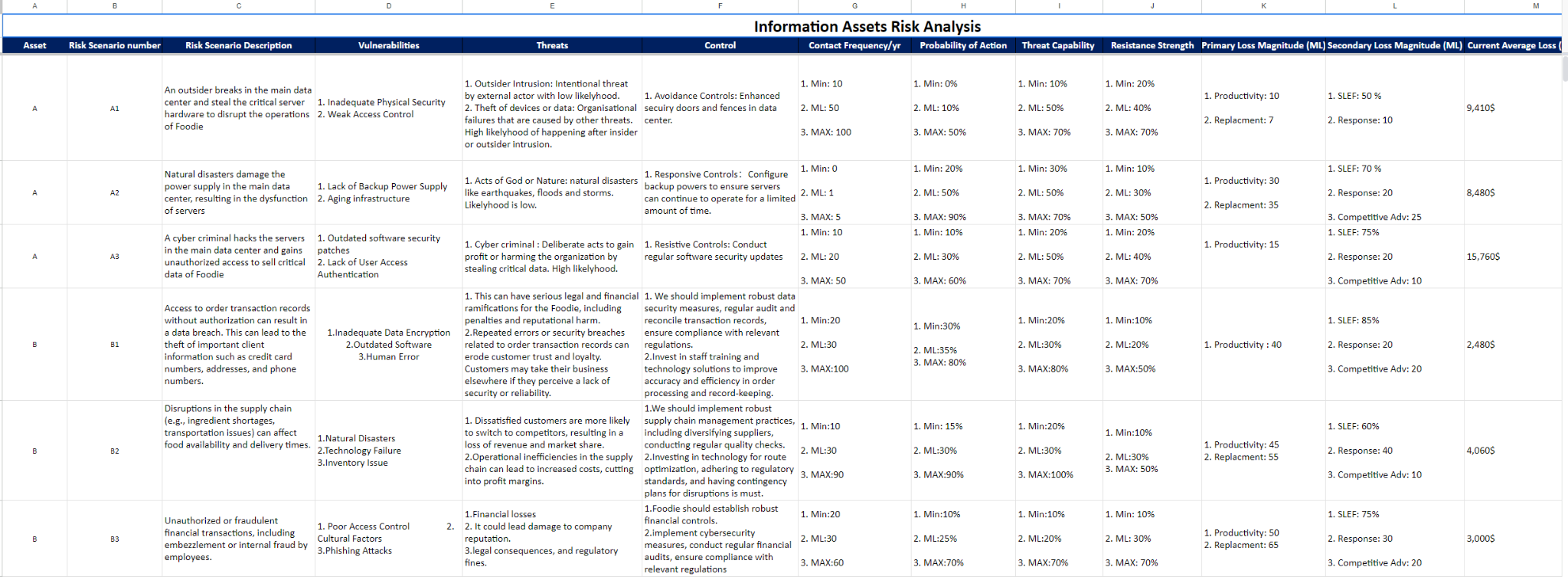
*Figure 2.a. Old WWMD and Consequence Table*



*Figure 2.b. New WWMD and Consequence Table*



*Figure 3.a. Old Information Assets Threat Risk Analysis Table*



*Figure 3.b. New Information Assets Threat Risk Analysis Table with OpenFair*

A screenshot of a computer

Description automatically generated

*Figure 3.c. New Information Assets Threat Risk Analysis Table with BIA*

## Major conflicts and decision-making

The management team discussed how many risk ratings we should have. Considering Foodie is only a start-up food delivery company, we decided to not make things too complicated and went with 5 risk ratings ranging from negligible to critical. Some of the management team members proposed using SLE to conduct cost of loss calculation. However, this decision was not agreed to by all the management team members. We decided to make a final decision once we have a better understanding of this area of knowledge. In week07, the management team agreed to separate and redesign the risk analysis table from the information assets identification table.

After week 08, the group learnt better approach to risk loss calculation which is OpenFair risk Analytic tool. We decided to use it to replace SLE and improve loss calculation. A screenshot of a computer

Description automatically generated

# Risk Evaluation

To properly determine the significance of the identified risks and prioritize them, the following processes have been implemented.

* Identification of risk tolerance/risk appetite in WWMD table
* Evaluation of business continuity

**Risk appetite:** To properly define risk appetite in Foodie’s risk management process, Foodie’s strategic business goal and its core business activities needs to be considered. Considering Foodie’s core business activity is food delivery service. The constant availability of such services is crucial as they directly affect customers’ satisfaction level. In WWMD table, we defined medium risk as “Medium risks are generally considered to be tolerable if there are only around 25% of the daily delivery services are disrupted insignificantly, a primary productivity loss less than 15, or a single total financial loss less than 5,000$. Pre-defined processes and procedures should be in place to help guide to control the potential damage if such a level of risk happens. No senior managers are required for assessment and monitoring unless the situation gets worse and unpredictable. Standard business operations can proceed with when such risks are properly controlled.” Around 25% of the daily delivery services are disrupted insignificantly which means the food delivery service is still operating at an acceptable level. High level risk which is one level above medium risk disrupts more 50% of the daily delivery services which is unacceptable at this point. Hence, we define risks from medium to negligible to be tolerable.

Relevant evidence can also be found in figure 2.b, WWMD table.

**Business continuity:** In the document “Foodie- Business Continuity Plan”, we linked the business continuity assessment back to the BIA in the TRA table. By conducting BIA and evaluating the impact on Foodie’s business continuity, we identified the critical information assets that need to be properly controlled by relevant policies and procedures. Figure 4.a and 4.b shows the Business Continuity Risk Assessment and Business Continuity Plan Development in the document “Foodie- Business Continuity Plan”.

A screenshot of a document

Description automatically generated

*Figure 4.a. Business Continuity Risk Assessment*

A white paper with black text

Description automatically generated

*Figure 4.b. Business Continuity Plan Development*

## Major conflicts and decision-making

The management team had some arguments about at which risk rating the risks are considered tolerable or intolerable. To decide on this, we thoroughly analyzed the characteristics of the service that Foodie provides. We concluded that the availability or the consistency of our food delivery service is crucial for both customer satisfaction and business success. This means that risks that can cause a noticeable degree of disruption to the food delivery service should be considered intolerable. According to our WWMD table, risk ratings that are equal or higher than medium will cause disruptions to the service. Hence, medium, high, and critical risks are considered intolerable, and the risk ratings below are considered tolerable depending on the circumstances.

# Review and Update log

To ensure that our risk management processes are up-to-date, effective, and aligned with Foodie’s business objectives, a review and update log is used to keep the historical record of changes, additions, or deletions in the risk assessment system. This will help the company achieve better accountability and traceability, and better compliance with ISO 27001.

| Entry # | Date & Time | Updated by | Reasons for update | Change description |
| --- | --- | --- | --- | --- |
| 1 | 08/09/2023 | CIO: Guangye Li | To have better document design | A new table and a new section have been added to the excel sheet “Foodie ISMS Table” |
| 2 | 30/09/2023 | 1. Template set up by CIO: Guangye Li  2. Content updated by All members | To have a better understanding of potential loss of Foodie’s critical information assets. | New and improved loss calculations using OpenFair risk analytics tool. |
| 3 | 07/10/2023 | 1. Template set up by CIO: Guangye Li  2. Content updated by All members | To have a better understanding of the potential impact of Foodie’s critical information assets risks on the business continuity. | Business impact analysis is integrated in the TRA table in “Foodie ISMS tables”. |
| 4 | 07/10/2023 | CIO: Guangye Li | To provide a structured and systematic approach to ensure the continuous delivery service of Foodie | Business continuity plan document is created. |
| 5 | 10/10/2023 | CIO: Guangye Li | To better integrate WWMD and Consequence table in the risk management process. | Improved WWMD and Consequence table with quantitative information. |
| 6 | 15/10/2023 | CIO: Guangye Li | To better categorize Foodie’s critical information assets and protect their CIA | Information classification policy is created, and information assets are classified accordingly. |