Foodie Information Security Risk Management Process Documentation

In accordance with ISO 27001, ISO 27005

# Purpose

This document outlines Foodie's risk management process, utilizing risk assessment and treatment, to ensure that the potential risks in our operations are effectively identified, analyzed, and mitigated. It covers all Foodie operations, from supply chain management to customer data handling and service delivery.

# Risk Management Strategy

At Foodie, we've built our risk management strategy on essential steps to make sure it is effective. We begin the risk management process by a clear establishment of our operational context and alignment with our strategic goals. Potential risks are identified, evaluated for their likelihood and impact, and then estimated in terms of their potential damage. Based on these insights, appropriate risk treatment plans are developed. Throughout this process, we integrate the Deming Cycle's principles of "Plan-Do-Check-Act" for continuous improvement. This ensures not only the identification and mitigation of risks but also the iterative enhancement of our strategies. Furthermore, the entire process is subject to ongoing monitoring and periodic reviews, ensuring our approach remains dynamic and responsive to the ever-evolving business environment.

# Context Establishment

Foodie's risk management starts by understanding the purpose and aligning with strategic objectives. We set clear boundaries and define our scope to ensure every risk, big or small, within our operations gets due consideration. By setting a clear operational baseline, Foodie is better equipped to identify deviations or threats, allocate resources efficiently, and communicate risk-related matters with clarity and relevance across the organization.

**Risk Management Scope:** Foodie's risk management scope encompasses its entire operations, from routine tasks like order handling and delivery to strategic initiatives and market growth endeavors. Specifically, it will manage the potential threats of Foodie’s critical information assets identified from critical business activities.

**Foodie’s strategic goals and internal context:** Foodie’s strategic goals and its internal context is identified in the document “Company Information & Business model”.

# Risk Assessment

At Foodie, our commitment to seamless service and operational excellence is underscored by our proactive approach to potential challenges. The purpose of conducting risk assessments as part of our risk management strategy is to systematically identify and evaluate potential threats that could hinder our objectives. Through thorough risk assessments, we gain crucial insights into the vulnerabilities within our operations, allowing us to anticipate, prepare for, and respond to various scenarios. It empowers us to make informed decisions, prioritize resources, and continuously refine our strategies for better outcomes. It can be divided into three main processes:

1. Risk Identification
   1. Identification of major information assets
   2. Identification of the risk scenarios of the major information assets
   3. Assignment of information assets’ owner
   4. Identification of information assets’ classification and labeling
2. Risk Estimation
   1. Threat Risk Analysis Table (See “Foodie ISMS Table”).
   2. OpenFair risk analytics tool.
   3. WWMD Table.
   4. Consequence Table.
   5. BIA
3. Risk Evaluation
   1. Risk Appetite.
   2. BCP

Complete Risk Assessment process is located in the document “Risk Assessment Document”.

# Risk Treatment

The purpose of risk treatment in our risk management strategy is to meticulously devise and implement actions that tackle the identified risks, ensuring that they are either mitigated, transferred, accepted, or avoided, based on their nature and potential impact. Main processes include:

1. Risk Treatment Plan
   1. Risk Treatment Decision Process
   2. Risk Treatment Options Selection
      1. How the controls are selected:
      2. Risk Retention
      3. Risk Reduction
      4. Identified Risk Controls
      5. Residual Risks
2. SOA
   1. Status of Applicability
   2. Explanation of selected controls

Complete Risk Assessment process is located in the document “Foodie Information Risk Treatment plan”.

# Plans for new Information Assets Management Procedure

To ensure that new information assets are introduced into our systems and processes safely and in alignment with Foodie's overarching risk management strategy.

* Asset Identification and Categorization: Upon introduction, each new information asset will be identified and categorized based on its criticality, sensitivity, and intended use. If the new assets are critical, they will be added to the information assets list in “Foodie ISMS Tables”. Information classification will help in tailoring specific risk management procedures for each asset.
* Risk Assessment: Follow the same procedures identified in the document “Risk Assessment Document”.
* Risk Treatment: Follow the same procedures identified in the document “Foodie Information Risk Treatment Plan”.
* Continuous monitoring and review.

# Integration of Deming Cycle: Check

This step validates the effectiveness of implemented risk controls, ensuring they effectively mitigate or manage identified risks. By comparing actual outcomes with anticipated results, discrepancies or gaps are identified, helping Foodie in preventing larger issues in the future.

* Feedback Mechanisms:
  + Engage stakeholders, including employees, suppliers, and customers, to gather feedback on the risk management initiatives. This provides a holistic understanding of how effective the measures are from multiple perspectives.
* Audit and Review:
  + Conduct internal audits to assess the effectiveness of the risk management process and to ensure compliance with internal standards and external regulations.
  + Review findings from audits, which provide an objective assessment of the risk controls and their effectiveness.
* Documentation and Reporting:
  + Document findings, insights, and learnings during the "Check" phase. This serves as evidence for compliance purposes and provides valuable insights for future risk management efforts.
  + Generate reports summarizing the outcomes of the "Check" phase (Foodie’s Evidence of Nonconformities), highlighting successes, areas of concern, and recommendations.

# Integration of Deming Cycle: Act on Monitoring and Review

In the Act phase of Foodie's risk management process, any shortcomings, or inefficiencies highlighted during the "Check" phase are addressed. By addressing inefficiencies, it ensures that Foodie's risk management process remains effective and relevant.

* Refinement: Based on the findings from the 'Check' phase, Foodie would refine its strategies. This could mean adjusting a particular process, introducing new technologies, or even revisiting the risk assessment if new risks emerge.
* Continuous Improvement: Always look for ways to make the risk management process more efficient and effective. This means regularly updating risk assessments, being proactive in identifying new potential threats, and ensuring that the organization is always prepared.

| Entry # | Date & Time | Updated by | Reasons for update | Change description |
| --- | --- | --- | --- | --- |
| 1 | 19/10/2023 | CIO: Guangye Li | To better manage new information assets added | Add new policy and procedure for new information assets’ risk management. |
| 2 | 21/10/2023 | CIO: Guangye Li | To have better risk treatment policy | Rework risk treatment plan |
|  |  |  |  |  |
|  |  |  |  |  |