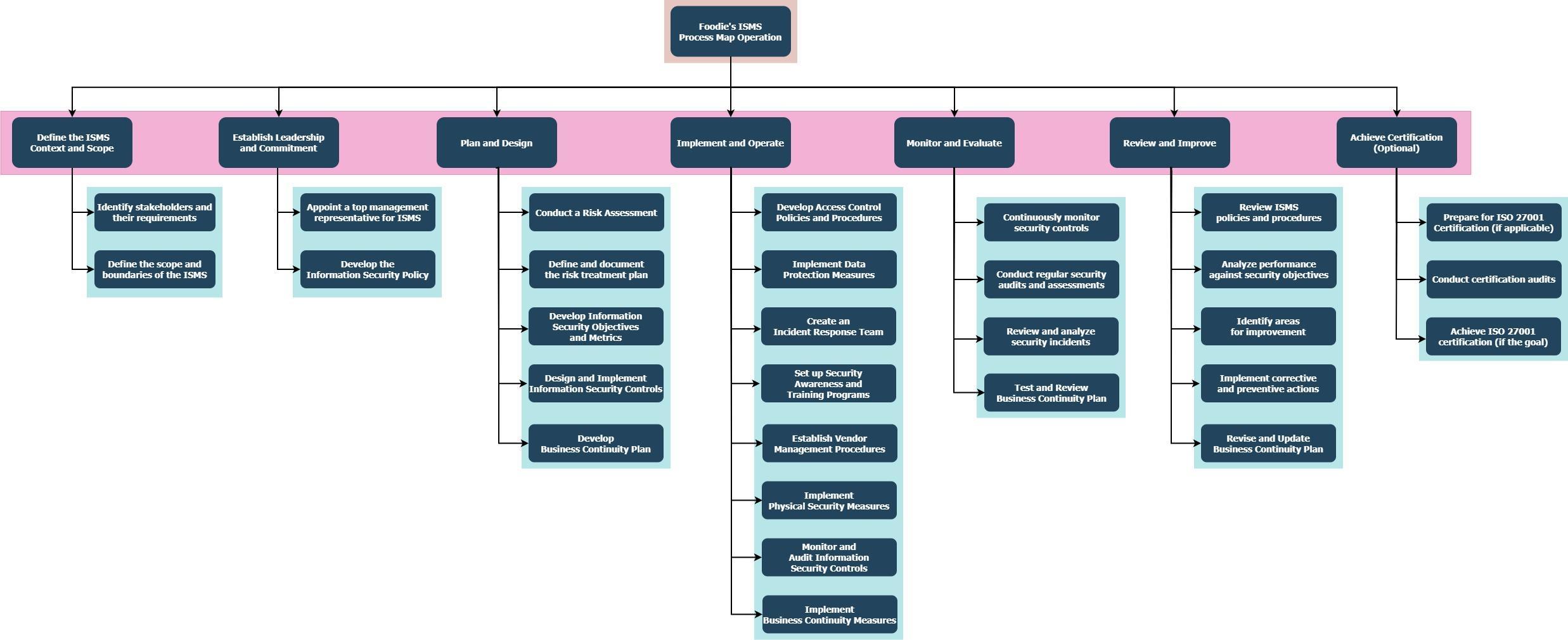
**``Foodie’s ISMS Process Map Operation**

****

# Foodie Scope of ISMS

Foodie's ISMS applies to its entire digital food delivery operations, covering the end-to-end process of food ordering, processing, delivery, and customer feedback. The scope encompasses the organization's primary administrative office located in Sydney, all digital assets including the customer-facing app, order management systems, payment system, backend servers and third-party integrations, as well as the physical infrastructure used by the employees and delivery personnel such as administrative office, database centre and warehouse. The ISMS is designed to protect the personal, financial, and transactional information of our customers, partners, and employees. Our business processes, from customer order placement to order fulfilment and delivery, fall under this ISMS. The ISMS is specifically aligned with Foodie's commitment to ensuring user trust, ensuring data privacy, and maintaining operational integrity in accordance with ISO 27001 and PCI DSS standards.

**Foodie’s ISMS Process Map Operation**

|  | **ISMS Process** | **Responsible** | **Description** | **Documentation** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| **Define the ISMS Context and Scope** | | | | |  |
|  | Identify stakeholders and their requirements | CEO (Chief Executive Officer)/ Head of Governance | Identify stakeholders, such as customers, delivery drivers, partners, regulatory agencies, and internal departments. Understand their specific requirements and expectations regarding data security, service availability, and privacy. | Stakeholder Requirements Document ***(Please refer to Company Informatin \_ Business model.docx)*** |  |
|  | Define the scope and boundaries of the ISMS | CEO (Chief Executive Officer)/ Head of Governance | Clearly outline the scope of the ISMS by specifying which systems, processes, and data are included. This should cover order processing systems, customer databases, payment gateways, and other critical components. Defining the boundaries ensures that all relevant aspects of Foodie's operations are protected. | ISMS Scope Statement ***(Please refer to Security Assessment Documentation)*** |  |
| **Establish Leadership and Commitment** | | | | |  |
|  | Appoint a top management representative for ISMS | CEO (Chief Executive Officer)/ CSO (Chief Security Officer) | Designate a senior executive, often the Chief Information Officer (CIO) or Chief Security Officer (CSO), as the top management representative for the ISMS. This person is responsible for providing leadership, allocating necessary resources, and ensuring that the ISMS is integrated into the overall business strategy. | Top Management Representative Appointment Document  ***(Please refer Foodie ISMS Tables - Evidence of the competence)*** | ***Foodie ISMS Tables - Evidence of the competence*** ensures that top management representatives and key personnel have the necessary competence to lead the ISMS. |
|  | Develop the Information Security Policy | CFO (Chief Financial Officer)/ CSO (Chief Security Officer) | Create a comprehensive Information Security Policy specific to the food delivery hub. This policy should outline the organization's commitment to safeguarding customer data, ensuring secure transactions, and maintaining the availability of services. It serves as the foundation for all security-related activities. | Information Security Policy ***(Please refer to Security Assessment Documentation and Foodie ISMS Tables - Evidence of the competence)  Note:*** *Ensuring that top management representatives and key personnel have the necessary competence to lead the ISMS.* |  |
| **Plan and Design** | | | | |  |
|  | Conduct a Risk Assessment | CFO (Chief Financial Officer)/ CTO (Chief Technology Officer) | Identify and evaluate risks associated with the food delivery operations. Consider risks related to data breaches, service interruptions, cyber-attacks, and regulatory compliance. The risk assessment provides the basis for implementing appropriate security measures. | Risk Assessment Report ***(Please refer to the following documents: - Risk Assessment Document.docx  - Foodie Financial Report.docx - Foodie ISMS Tables - Information Assets List - Foodie ISMS Tables - Threat Risk Analysis - Foodie ISMS Tables - Business Impact Analysis - Foodie ISMS Tables - WWMD and Consequence Table)*** | ***Foodie Financial Report.docx*** is used in this step to assess the financial implications of identified risks, including potential losses, costs associated with security incidents, and the financial impact of security controls needed to mitigate these risks.  ***Foodie ISMS Tables - Information Assets List*** is used in this step to identify and catalog all information assets that the food delivery processes, stores, or transmits. This list is a fundamental component of the risk assessment process, as it helps in understanding what needs to be protected and assessing the associated risks.This list includes details about the assets, such as their names, descriptions, classifications, ownership, and sensitivity levels.  ***Foodie ISMS Tables - Threat Risk Analysis*** is used in this step to identify and analyze potential threats that could impact the organization's information assets and information security. It assesses the likelihood of threats occurring and the potential impact they may have on the organization.  ***Foodie ISMS Tables - Business Impact Analysis*** is used in this step to assess the criticality of business processes, functions, and information assets. It helps in understanding the potential impact of disruptions, incidents, or security breaches on the organization's core operations and services.  ***Foodie ISMS Tables - WWMD and Consequence Table*** are used in this step to assess and prioritize risks. The WWMD table helps in considering how management would respond to different risk scenarios, while the Consequence Table is used to evaluate the potential consequences of various risks on the organization's operations and objectives. |
|  | Define and document the risk treatment plan | CFO (Chief Financial Officer)/ CTO (Chief Technology Officer) | Develop a risk treatment plan that outlines strategies for mitigating identified risks. Specify control measures, contingency plans, and incident response procedures. This plan guides the implementation of security controls to minimize vulnerabilities. | Risk Treatment Plan ***(Please refer to Foodie Information Risk Treatment plan.docx)*** |  |
|  | Develop Information Security Objectives and Metrics | CIO (Chief Information Officer) | Establish specific security objectives that align with the business goals of Foodie's organization. Define measurable metrics to assess the effectiveness of security controls. These objectives provide a clear direction for the ISMS implementation and enable performance evaluation. | Objectives and Metrics Document ***(Please refer to Security Assessment Documentation)*** |  |
|  | Design and Implement Information Security Controls | CTO (Chief Technology Officer) | Design and deploy a set of security controls tailored to the food delivery industry. These controls may include encryption protocols, access management systems, secure coding practices, and network security measures. Implementation ensures the protection of sensitive data and critical systems. | Security Control Implementation Plan ***(Please refer to Security Assessment Documentation and Foodie The Statement of Applicability)*** | ***Foodie The Statement of Applicability*** (SoA) is used in this step to identify and document the specific information security controls that are applicable and necessary to food delivery operations. It outlines which controls will be implemented to address identified risks and protect information assets. |
|  | Develop Business Continuity Plan | COO (Chief Operation Officer) | Create a comprehensive Business Continuity Plan (BCP) specific to Foodie's organization. The BCP outlines procedures for maintaining essential services during disruptions, such as natural disasters or cyber incidents. It includes strategies for data recovery, service restoration, and communication with stakeholders. | Business Continuity Plan  ***(Please refer to Foodie- Business Continuity Plan)*** |  |
| **Implement and Operate** | | | | | Providing evidence that staff responsible for developing and implementing security controls, managing access, and responding to incidents are competent in their roles. |
|  | Develop Access Control Policies and Procedures | CTO (Chief Technology Officer)/ CSO (Chief Security Officer) | Establish access control policies defining user privileges, authentication methods, and authorization processes. Implement procedures for granting and revoking access rights based on roles and responsibilities. Access control ensures that only authorized personnel can access sensitive systems. | Access Control Policy, Access Control Procedures |  |
|  | Implement Data Protection Measures | CSO (Chief Security Officer) | Implement data protection measures, such as encryption, tokenization, and anonymization, to safeguard customer data. Ensure that data is protected both in transit and at rest. Data protection mechanisms prevent unauthorized access and data breaches. | Data Protection Policy |  |
|  | Create an Incident Response Team | CSO (Chief Security Officer) | Formulate an Incident Response Team (IRT) responsible for detecting, analyzing, and responding to security incidents. Define roles, responsibilities, communication channels, and incident escalation procedures. The IRT ensures a swift and effective response to security breaches. | Incident Response Plan, Incident Response Team Charter |  |
|  | Set up Security Awareness and Training Programs | CSO (Chief Security Officer)/ COO (Chief Operation Officer) | Develop security awareness programs and training materials for employees, contractors, and partners. These programs educate personnel about security threats, best practices, and the organization's policies. Regular training sessions enhance security awareness and promote a security-conscious culture. | Security Awareness Program Plan, Training Materials ***(Please refer to Foodie ISMS Tables - Evidence of the competence)*** | ***Foodie ISMS Tables - Evidence of the competence*** contains competence of individuals responsible for security awareness and training programs. |
|  | Establish Vendor Management Procedures | CSO (Chief Security Officer)/ Head of Governance | Implement procedures for evaluating, selecting, and monitoring third-party vendors. Vendor management ensures that external partners meet security standards and comply with contractual obligations. Assess the security posture of vendors to minimize supply chain risks. | Vendor Management Policy, Vendor Assessment Forms |  |
|  | Implement Physical Security Measures | CSO (Chief Security Officer)/ COO (Chief Operation Officer) | Deploy physical security measures to protect data centers, server rooms, and other critical facilities. Physical security controls include surveillance systems, access barriers, biometric authentication, and environmental controls. Physical security safeguards against unauthorized access and physical threats. | Physical Security Policy |  |
|  | Monitor and Audit Information Security Controls | CSO (Chief Security Officer)/ CFO (Chief Financial Officer) | Continuously monitor the effectiveness of security controls. Conduct regular security audits and assessments to identify vulnerabilities, compliance gaps, and emerging threats. Audits help maintain the integrity of security measures. | Monitoring and Audit Plan, Audit Reports |  |
|  | Implement Business Continuity Measures | COO (Chief Operation Officer) | Put into operation the strategies and measures outlined in the Business Continuity Plan (BCP). These measures ensure that the food delivery hub can maintain critical services and data availability during disruptions. Regular testing and exercises validate the BCP's effectiveness. | Business Continuity Plan Implementation Reports |  |
| **Monitor and Evaluate** | | | | |  |
|  | Continuously monitor security controls | CTO (Chief Technology Officer) | Implement continuous monitoring systems that provide real-time visibility into the performance of security controls. Continuous monitoring ensures the timely detection of security incidents and anomalies. | Continuous Monitoring Reports  ***(Please refer to Evidence of nonconformities identified and corrective actions arising.docx)*** | In this step, evidence of nonconformities identified during security control monitoring is recorded and documented. Corrective actions may arise from the identification of these nonconformities. |
|  | Conduct regular security audits and assessments | CFO (Chief Financial Officer) | Regularly perform comprehensive security audits and assessments to evaluate the overall security posture. These evaluations identify areas for improvement and help maintain compliance with industry standards. | Security Audit Reports  ***(Please refer to Evidence of nonconformities identified and corrective actions arising.docx*** | During security audits and assessments, evidence of nonconformities related to security controls, policies, or procedures may be identified and documented. Corrective actions are initiated based on these findings. |
|  | Review and analyze security incidents | CSO (Chief Security Officer) | Review all security incidents that occur in Foodie's organization. Conduct in-depth analysis and root cause assessments to identify lessons learned and improve incident response procedures. | Security Incident Reports  ***(Please refer to Evidence of nonconformities identified and corrective actions arising.docx*** | Evidence of nonconformities identified during the review and analysis of security incidents, such as breaches or incidents, is documented. Corrective actions may be necessary to address the root causes of these incidents. |
|  | Test and Review Business Continuity Plan | COO (Chief Operation Officer) | Periodically test the effectiveness of the Business Continuity Plan (BCP). Conduct exercises and simulations to evaluate the plan's readiness to address different types of disruptions. Review and update the BCP based on the results of tests. | Business Continuity Plan Testing and Review Reports |  |
| **Review and Improve** | | | | |  |
|  | Review ISMS policies and procedures | Head of Governance | Conduct regular reviews of ISMS policies and procedures to ensure they remain aligned with the evolving threat landscape and organizational changes. Updates should reflect lessons learned from incidents and changing industry regulations. | Policy and Procedure Review Reports  ***(Please refer to Evidence of nonconformities identified and corrective actions arising.docx*** | During the review of ISMS policies and procedures, evidence of nonconformities related to policy compliance or procedural issues may be identified. Corrective actions are implemented to address these nonconformities. |
|  | Analyze performance against security objectives | CSO (Chief Security Officer)/ CIO (Chief Information Officer) | Assess the organization's performance against defined security objectives and metrics. Analyze the results to identify areas for improvement and align security measures with the organization's strategic goals. | Performance Analysis Reports  ***(Please refer to Evidence of nonconformities identified and corrective actions arising.docx*** | Evidence of nonconformities related to performance against security objectives is documented during this step. Corrective actions are taken to improve performance. |
|  | Identify areas for improvement | CSO (Chief Security Officer)/ CIO (Chief Information Officer) | Based on performance analysis and incident reviews, identify areas where security can be enhanced. These areas may include process improvements, control enhancements, and employee training. | Areas for Improvement Report |  |
|  | Implement corrective and preventive actions | CSO (Chief Security Officer)/ CIO (Chief Information Officer) | Develop and implement action plans to correct security deficiencies and prevent the recurrence of incidents. Corrective actions address existing security issues, while preventive actions aim to avoid future problems. | Corrective and Preventive Action Plans  ***(Please refer to Evidence of nonconformities identified and corrective actions arising.docx*** | In this step, corrective actions arising from the identification of nonconformities are documented and implemented to address the root causes of nonconformities. |
|  | Revise and Update Business Continuity Plan | CSO (Chief Security Officer)/ COO (Chief Operation Officer) | Regularly review, revise, and update the Business Continuity Plan (BCP) to address changing risks, business processes, and lessons learned from tests and real incidents. The BCP should evolve to ensure the continued resilience of the organization. | Business Continuity Plan Revisions and Updates |  |
| **Achieve Certification (Optional)** | | | | |  |
|  | Prepare for ISO 27001 Certification (if applicable) | CIO (Chief Information Officer) | If ISO 27001 certification is a goal, prepare the organization by aligning ISMS practices with ISO 27001 requirements. This involves conducting a gap analysis, addressing identified gaps, and preparing the organization for certification audits. | ISO 27001 Certification Preparation Plan |  |
|  | Conduct certification audits | CIO (Chief Information Officer) | Engage with a certification body to conduct audits to assess the organization's compliance with ISO 27001 standards. These audits evaluate the effectiveness of ISMS practices. | Certification Audit Plans ***(Please refer to Foodie ISMS Tables - Evidence of the competence)*** | Demonstrating competence and compliance with ISO 27001 or other relevant standards during certification audits. |
|  | Achieve ISO 27001 certification (if the goal) | CIO (Chief Information Officer) | After successfully completing certification audits, the organization achieves ISO 27001 certification, demonstrating its commitment to information security and compliance with international standards. | ISO 27001 Certification |  |