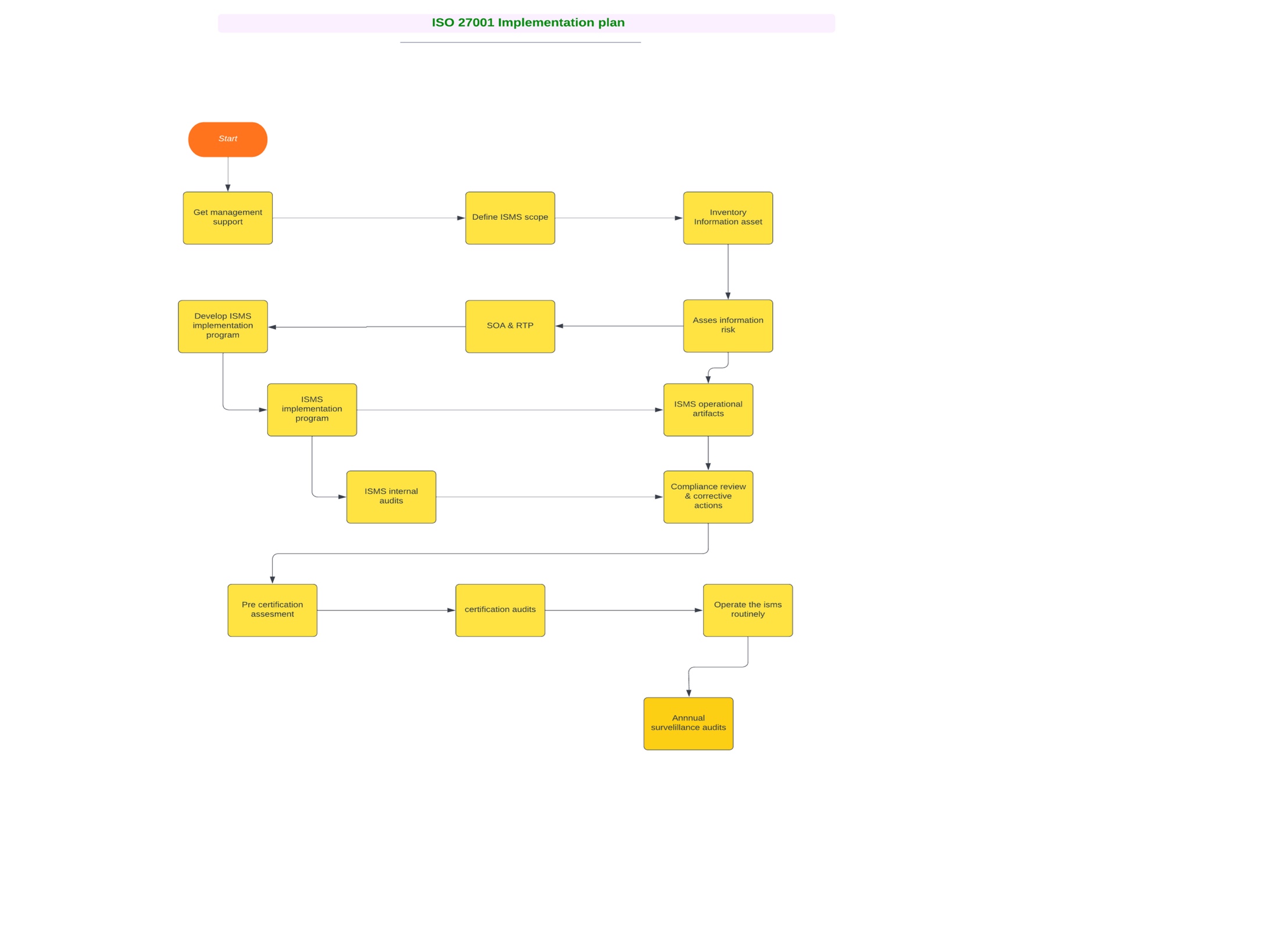
ISO 27001 Implementation Plan for a Food Delivery Company



The image provides an overview of the practical deliverables related to the Information Security Management System (ISMS) in the context of ISO standards.

**Get Management Support:**

* + At first, we Secure endorsement from company executives.
  + Getting the importance of information security for the FOODIE business, especially with regards to customer data and payment information.

**Define ISMS Scope:**

* + Here, we Focus on areas like customer data management, payment gateway integration, vendor information, mobile app and website security, and employee data management.

**Inventory Information Assets:**

* + We took assets like customer databases, payment gateways, mobile apps, website, vendor management systems, and internal communication platforms.

**Assess Information Risks:**

* + Here, we Identify potential risks such as data breaches, payment frauds, vendor information leaks, and app and website vulnerabilities.

**Prepare Statement of Applicability (SOA) & Risk Treatment Plan (RTP):**

* + Here we decide which controls from ISO 27001 apply to our company.
  + We then develop a plan detailing how identified risks will be managed or mitigated.

**Develop ISMS Implementation Program:**

* + It used for securing customer data, ensuring secure payment processes, vetting third-party vendors for security compliance, and ensuring app/website security.

**ISMS Implementation Program:**

* + Here for executing the above plan, which might involve improving encryption, conducting regular security audits, employee training, and vulnerability assessments.

**ISMS Operational Artefacts:**

* + We here create and manage some documents like security policies, incident response plans, and vendor compliance reports.

**ISMS Internal Audits:**

* + It is used to Conduct internal checks focusing on areas like payment gateway security, customer data protection, and mobile app security.

**Compliance Review & Corrective Actions:**

* Used for regularly review for adherence to ISO 27001 and take corrective actions where needed.

**Pre-certification Assessment & Certification Audit:**

* It may use to engage an external auditor to evaluate the ISMS before the final certification.

**Operate the ISMS Routinely & Annual Surveillance Audits:**

* It partially used to ensure ongoing operation and conduct regular audits to ensure continued ISO 27001 compliance.