# ISO 27001 Compliant Capital Planning and Investment Control (CPIC) Process Template

## Introduction:

This document describes the Capital Planning and Investment Control (CPIC) process required for ISO 27001 compliance. The CPIC process ensures systematic and strategic decision-making for information security investments, enabling [COMPANY NAME] to align its financial resources with the goals and objectives of the Information Security Management System (ISMS).

## 1. Purpose of the CPIC Process

The CPIC process aims to:  
1. [Insert purpose statement here.] (e.g., Ensure financial resources are aligned with ISMS objectives.)  
2. [Insert purpose statement here.] (e.g., Prioritize investments based on risk assessment outcomes.)  
3. [Insert purpose statement here.] (e.g., Maintain compliance with regulatory requirements.)  
4. [Insert purpose statement here.] (e.g., Improve the efficiency of resource allocation for security initiatives.)  
5. [Insert purpose statement here.] (e.g., Support continuous improvement in information security practices.)

## 2. CPIC Process Flowchart

(Insert Flowchart Here)

Flowchart Description:

* Initiation:  
  Triggered by [insert trigger]. (e.g., identification of new regulatory requirements or audit findings.)  
  Key Inputs: [insert key inputs]. (e.g., risk assessments, incident reports, or strategic goals.)
* Requirement Definition:  
  Define [insert details]. (e.g., scope, objectives, and desired outcomes for the investment.)  
  Stakeholders: [insert stakeholders]. (e.g., ISM, department heads, and IT Operations.)
* Feasibility Analysis:  
  Evaluate [insert evaluation criteria]. (e.g., technical, operational, and financial feasibility.)  
  Key Outputs: [insert key outputs]. (e.g., cost-benefit analysis and feasibility report.)
* Approval and Prioritization:  
  Present findings to [insert responsible group]. (e.g., Information Security Committee.)  
  Investments are prioritized based on [insert prioritization criteria]. (e.g., risk severity, regulatory urgency, and resource availability.)
* Implementation Planning:  
  Develop [insert plan details]. (e.g., a detailed timeline, budget, and resource allocation plan.)  
  Responsible Party: [insert responsible party]. (e.g., Project Management Office in collaboration with ISM.)
* Execution:  
  Implement [insert execution details]. (e.g., execute the approved project steps and track progress.)  
  Key Outputs: [insert key outputs]. (e.g., progress reports and performance metrics.)
* Monitoring and Evaluation:  
  Regularly monitor [insert monitoring details]. (e.g., performance against ISMS objectives.)  
  Conduct post-implementation reviews to [insert objectives]. (e.g., identify lessons learned and measure success.)
* Feedback Loop:  
  Use [insert evaluation findings] to improve future CPIC processes. (e.g., incorporate feedback into process refinements.)

## 3. Roles and Responsibilities

Chief Executive Officer (CEO):  
[Insert responsibilities here.] (e.g., Provide final approval for significant investments.)

Chief Information Security Officer (CISO):  
[Insert responsibilities here.] (e.g., Oversee CPIC process and ensure alignment with ISMS.)

Information Security Committee (ISC):  
[Insert responsibilities here.] (e.g., Review and prioritize proposed investments.)

Information Security Manager (ISM):  
[Insert responsibilities here.] (e.g., Facilitate risk assessments and define investment requirements.)

Project Management Office (PMO):  
[Insert responsibilities here.] (e.g., Develop and manage project plans for approved investments.)

Finance Team:  
[Insert responsibilities here.] (e.g., Ensure budgetary compliance and monitor financial performance.)

## 4. Narrative Context

The CPIC process enables [COMPANY NAME] to maintain a strategic approach to managing information security investments. This structured process ensures that financial resources are allocated effectively to mitigate risks, enhance compliance, and achieve ISMS objectives. By continuously monitoring and evaluating investments, the organization can drive ongoing improvements and adapt to evolving threats.

[Insert additional context here.] (e.g., Describe a scenario where the CPIC process successfully resolved a critical information security issue.)

## 5. Revision and Maintenance

This document and the CPIC process will be reviewed [insert frequency] or as needed to reflect changes in organizational priorities, regulatory requirements, or the threat landscape.

## Approval:

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |