# ISO 27001 Capital Planning and Investment Policy Template

# 1. Introduction

This document outlines the Capital Planning and Investment Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes a framework for managing financial resources allocated to capital investments in a manner that supports the organization’s information security objectives.

# 2. Purpose

The purpose of this policy is to:

- Ensure that capital planning and investments align with the organization’s strategic goals and risk management practices.

- Define roles and responsibilities for capital planning and investment activities.

- Establish processes for prioritizing, approving, and monitoring capital expenditures.

- Enhance accountability and transparency in the allocation and use of financial resources.

# 3. Scope

This policy applies to all capital planning and investment activities within [Organization Name]. It encompasses all departments, business units, and projects involving the acquisition, development, or enhancement of assets, including infrastructure, technology, and services.

# 4. Roles and Responsibilities

- Finance Department: Oversees the budgeting and financial management of capital investments, ensuring alignment with organizational priorities.

- Project Sponsors: Propose capital investment initiatives, develop business cases, and ensure projects deliver intended outcomes.

- Risk Management Team: Evaluates potential risks associated with capital investments and ensures mitigation strategies are implemented.

- Information Security Officer (ISO): Ensures that capital investments comply with ISO 27001 requirements and support information security objectives.

- Executive Leadership: Reviews and approves significant capital investments based on strategic alignment and risk assessments.

# 5. Capital Investment Planning Process

5.1 Identification

- Departments and business units identify capital investment needs based on operational requirements and strategic objectives.

- Investment proposals must include a business case, risk assessment, and expected benefits.

5.2 Prioritization

- Proposals are evaluated and prioritized based on criteria such as:

- Strategic alignment

- Risk impact

- Cost-benefit analysis

- Resource availability

5.3 Approval

- Capital investments require approval through established governance structures, such as an investment review board or executive committee.

- Approvals must be documented and retained for audit purposes.

5.4 Implementation

- Approved investments are executed in accordance with the project plan, ensuring compliance with procurement and information security policies.

5.5 Monitoring and Review

- Investment performance is monitored against defined metrics and milestones.

- Post-implementation reviews are conducted to assess the success and value delivered by the investment.

# 6. Risk Management

- All capital investments must undergo a risk assessment to identify potential threats to information security and organizational objectives.

- Mitigation plans must be developed and integrated into the investment planning process.

- High-risk investments require additional oversight and approval by the Risk Management Team.

# 7. Compliance and Reporting

- Compliance with this policy is mandatory for all employees and contractors involved in capital planning and investment activities.

- Periodic audits will be conducted to ensure adherence to the policy.

- Reports on capital investment performance and compliance must be submitted to executive leadership quarterly.

# 8. Policy Review

This policy will be reviewed annually or whenever significant changes occur in the organization’s operations, regulatory environment, or strategic objectives. Recommendations for updates will be considered by the Information Security Officer and executive leadership.

# 9. Acknowledgment

All employees and contractors involved in capital planning and investment activities must acknowledge receipt and understanding of this policy. Signed acknowledgment forms will be retained for audit purposes.

# Appendices

## Appendix A: Capital Investment Proposal Template

| Proposal ID | Project Name | Sponsor | Estimated Cost | Expected Benefits | Risk Assessment |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Appendix B: Post-Implementation Review Template

| Review ID | Project Name | Key Metrics | Outcomes | Lessons Learned | Recommendations |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Appendix C: Policy Acknowledgment Form

I acknowledge that I have read and understood the Capital Planning and Investment Policy and agree to comply with its requirements.  
  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_