# ISO 27001 IT Business Decision Process Template

## Introduction:

This document outlines the IT Business Decision Process for [COMPANY NAME] in compliance with ISO 27001 standards. It ensures that decisions involving IT investments, strategies, and operations align with the organization’s Information Security Management System (ISMS) and its objectives of confidentiality, integrity, and availability of information assets.

## 1. Purpose of the IT Business Decision Process

The purpose of the IT Business Decision Process is to:  
1. Align IT decisions with business objectives and strategic goals.  
2. Mitigate risks to information assets and ensure compliance with legal, regulatory, and contractual obligations.  
3. Optimize resources by prioritizing IT investments based on business needs and risk impact.  
4. Foster continuous improvement by evaluating and refining IT strategies and processes.

## 2. Decision Criteria

Each IT business decision will be evaluated based on the following criteria:

* 1. Financial Feasibility: Evaluate cost-effectiveness and return on investment (ROI).
* 2. Risk Impact: Assess potential risks to information assets, systems, and processes.
* 3. Compliance Requirements: Ensure alignment with ISO 27001 controls and other legal or regulatory obligations.
* 4. Operational Efficiency: Determine how the decision enhances efficiency and performance.
* 5. Strategic Alignment: Verify alignment with organizational goals and long-term strategies.

## 3. IT Business Decision Process Flowchart

The process follows these stages:  
1. Initiation: Triggered by business requirements, security incidents, or strategic goals.  
2. Impact Analysis: Evaluate financial, technical, and security implications. Identify risks and potential mitigations.  
3. Approval: Submit the proposal to the Information Security Committee (ISC) or relevant stakeholders for review.  
4. Implementation Planning: Develop detailed plans for implementation, including timelines, resource allocation, and communication strategies.  
5. Execution: Carry out the approved decision with ongoing monitoring and reporting.  
6. Review and Feedback: Conduct a post-implementation review to evaluate outcomes and identify areas for improvement.

## 4. Post-Implementation Metrics

The following metrics will be used to evaluate the success of IT business decisions after implementation:

* Cost Savings: Measure the financial benefits achieved post-implementation.
* Risk Reduction: Assess the extent to which identified risks were mitigated.
* Performance Improvement: Evaluate operational efficiency and system performance enhancements.
* Compliance Success: Determine the decision's effectiveness in meeting compliance requirements.

## 5. Roles and Responsibilities

Top Management:  
- Approve major IT business decisions.  
- Ensure alignment of IT strategies with business objectives.

Information Security Manager (ISM):  
- Assess risks and compliance implications of IT decisions.  
- Provide input on security controls required for implementation.

IT Operations Team:  
- Execute approved decisions and implement technical solutions.  
- Monitor and report on progress and effectiveness of IT projects.

Finance Team:  
- Evaluate the financial feasibility of IT investments.  
- Ensure budgetary compliance and resource allocation.

Information Security Committee (ISC):  
- Review and approve IT business decisions.  
- Ensure decisions align with the ISMS and risk management framework.

## 6. Revision and Maintenance

This document will be reviewed [Insert frequency, e.g., annually or as needed] to reflect changes in the organization’s IT strategy, regulatory requirements, or threat landscape.

## Approval:

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