Contents

[1 Policy life cycle approach 1](#_Toc456961411)

[1.1 Plan which policies are required and the overall structure to be applied 2](#_Toc456961412)

[1.2 Design the required policies 2](#_Toc456961413)

[1.3 Implement the policies 2](#_Toc456961414)

[1.4 Operate / use the policies 2](#_Toc456961415)

[1.5 Evaluate/monitor the policies 3](#_Toc456961416)

[1.6 Update/dispose of the policies 3](#_Toc456961417)

[2 Recommended Policy structure 3](#_Toc456961418)

[2.1 Document header information 3](#_Toc456961419)

[2.2 Introduction 3](#_Toc456961420)

[2.3 Purpose 3](#_Toc456961421)

[2.4 Scope 3](#_Toc456961422)

[2.5 Roles and Responsibilities 3](#_Toc456961423)

[2.6 Sanctions and Violations 4](#_Toc456961424)

[2.7 Revisions and Updating Schedule 4](#_Toc456961425)

[2.8 Contact information 4](#_Toc456961426)

[2.9 Definitions/Glossary 4](#_Toc456961427)

[2.10 Acronyms 4](#_Toc456961428)

[3 Overall structure of the policy framework 5](#_Toc456961429)

[4 Sources 5](#_Toc456961430)

# Policy life cycle approach

This section explains the recommended overall policy life cycle.

## Plan which policies are required and the overall structure to be applied

**Detailed advice**—This phase establishes the foundation for a policy framework by covering the stakeholders and goals dimensions defined previously. Usually, organizations already have some policies in place; therefore, identifying gaps between the governance principles and current, valid policies helps to redesign and improve the policy framework in use. In this

phase, a logical structure of documentation that will support and clarify policy principles is defined. The optimal amount of documentation depends on the organization’s culture and

management’s style; the objective of this activity is to improve clarity of policy principles and support their implementation.

## Design the required policies

**Detailed advice** —There are two activities in this phase:

1. Priorities setup—Identification of concrete policies, using a risk-based approach that addresses policy principles, setting deadlines and priorities for their review or creation

2. Policy structure definition—Writing a policy is not only a writing activity; it needs adequate coordination, including:

− Policy draft—Identify the individuals responsible for researching and writing policies. A critical success factor is to resolve any potential issue concerning the feasibility for implementing policy principles.

− Policy review—Identify the individuals responsible for providing an independent review. The objective of this activity is to increase the policy credibility and quality.

− Approval, communication and distribution—Establish the procedure for obtaining final policy approval from the authorized individuals defined in the stakeholders dimension previously, and determine the policy communication and training strategy.

− Style—Define writing quality standards, including document format, font type, language style, glossary of terms and document structure. The objective of this activity is to ensure that policies are written, presented and structured in a way that is clear, concrete, complete, consistent and easy to follow.

## Implement the policies

**Detailed advice** —This activity corresponds to implementation and enforcement policies, defining activities that will assist the organization in providing a transparent transition from a noncompliant to a compliant state.

## Operate / use the policies

**Detailed advice** **—**An effective policy should be part of the organization’s DNA. Building an accountable culture and using policies in daily operations ensures that the organization’s goals are met. In this phase, organizations should “walk the talk” of policy principles.

## Evaluate/monitor the policies

**Detailed advice** **—**This phase has the objective to confirm that policy requirements are properly implemented and the organization operates effectively. The degree of success of

policy principles supporting business goals is evaluated, and the overall efficiency of the policy framework is communicated to relevant stakeholders.

## Update/dispose of the policies

**Detailed advice** **—**To keep policies aligned with business direction, policies are reviewed for updating or removal. This activity has two objectives: to ensure that organizations have effective policies and to adjust the phases defined previously to maintain or improve the maturity of the policy framework. Good practice would require policies to be reviewed on a regular basis, typically every 12 months.

# Recommended Policy structure

## Document header information

(conform to enterprise standards for document management)

## Introduction

This section should introduce the policy by name and locate it within the hierarchy of other existing information security and company policy documents.

## Purpose

State the main goals of the policy; this will explain the reason for the policy and will help readers understand how the policy should be used. Legal and compliance issues should also be mentioned in here. Include statements on any specific legislation the policy is designed to adhere to.

## Scope

The scope is a statement of the infrastructure and information systems to which the policy applies, and the people who are stakeholders in it. Stakeholders would typically include anyone who is a user of the information or systems covered by the policy.

## Roles and Responsibilities

This is a statement of the structures through which the responsibilities for policy implementation are delegated throughout the company. Job roles may be specified in this section, e.g., Database Administrators (DBAs), Technical Custodians, Field Office employees, etc.

## Sanctions and Violations

This section details to what extent breaking policy is considered a violation (e.g., it is HR-related and therefore related to an employee’s contract, or is it an information security department matter?) This section should also detail how violations should be reported, who to and what actions should be taken in the event of a violation. It should also include information on what sanctions will be carried out resulting from a violation (for example, verbal or written warnings, etc).

## Revisions and Updating Schedule

This section defines who is responsible for making updates and revisions to the policy and how often these will take place. It may be useful to include a reference to the document as a “living document” which can be updated as determined by those responsible for updates and revisions. This will ensure that any ad hoc revisions are accounted for as well as scheduled updates. Information should also be included detailing where the policy will be published and how employees can access it.

## Contact information

Detail who should be contacted in connection with policy. A group or mailbox rather than an individual is preferable here as these are less likely to change.

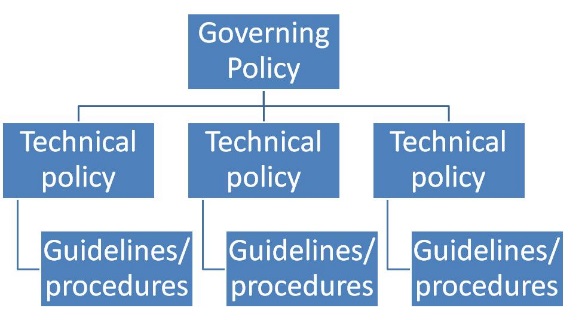
## Definitions/Glossary

Define any terms that may be unfamiliar to the reader. The necessity for this will depend on the audience, e.g., the readership of a Technical Policy for Linux are likely to already be familiar with the Linux technical terms, therefore it will not be necessary to spell these out. The cryptography section of the user policy however may include terms with which readers are not familiar and these should be defined in footnotes or a glossary to aid comprehension.

## Acronyms

A separate section spelling out acronyms may be required where there are a large number or where the document is long or complex. For shorter documents, acronyms may instead be spelt out in the body of the document.

# Overall structure of the policy framework



The core components of a policy framework are:

• Appointment of individuals who have the authority to approve policies and their associated responsibilities

• Determination of the consequences for failing to comply with given policies

• Definition of a process for handling exceptions to policies

• Definition of a method for measuring and monitoring compliance with policies

• Definition of the scope of the policy and the group of stakeholders that has to follow the policy

# Sources

* IT Policy Framework Based on COBIT 5, J Carillo *ISACA JOURNAL* VOLUME 1, 2013
* SANS Institute 2007, Information Security Policy - A Development Guide for Large and Small Companies
* www.InfoTech.com