iGUIDE

ISMS

Information Security Capability Maturity Model

iNFOSECBASE

Contents

A Guide to the Capability Maturity Model 3
Introduction 3
Maturity Levels and Attributes 3
CMM Descending Model Table 4
Key Areas 4
Assessment 4
Continual Improvement 4

A Guide to the Capability Maturity Model

Introduction

The Information Security Capability Maturity Model (CMM) is a framework that assesses and measures an organisation's maturity in managing information security. It provides a practical and structured approach for organisations to monitor their ISMS's effectiveness and identify areas for improvement.

One of the key principles of ISO 27001 is Continual Improvement; being able to demonstrate how you can continuously improve your ISMS is not only a requirement, but a huge advantage to having an ISO 27001 certified ISMS.

As your ISMS scales with your growing organisation, auditors would expect you to revise your controls and policies as the system matures or when a new process is implemented to identify opportunities for improvement. Determining if and how your organisation identifies improvement opportunities and potential system underperformance is essential to the longevity of your program.

To identify opportunities for improvement, you can continuously monitor the security of your systems and their operational performance in the following areas:

- Annex A controls
- Policies
- Procedures
- ISMS objectives

Maturity Levels and Attributes

The classifications for CMM Levels and Attributes are:

1. **Non-existent**: no controls, policies or procedures in place
2. **Initial/Ad Hoc**: control poorly deployed with non-documented strategies, manual management processes, and lack of integration with the other controls and systems.
3. **Repeatable**: processes supported by informal documentation and performed by personnel with mixed skill levels.
4. **Defined**: strategic management structure in place with well-defined documented processes supported by a trained team.
5. **Managed**: processes and controls aligned with the organizational strategic objectives.
6. **Optimised**: process performed at an optimal level and continuously monitored by top management.

CMM Descending Model Table

Level	Attribute	Description
5	Optimised	Process performed at an optimal level and continuously monitored by top management
4	Managed	Processes and controls aligned with the organisational strategic objectives
3	Defined	Strategic management structure in place with well-defined documented processes supported by a trained team
2	Repeatable	Processes supported by informal documentation and performed by personnel with mixed skill levels
1	Initial/Ad Hoc	Control poorly deployed with non-documented strategies, manual management processes, and lack of integration with the other controls and systems
0	Non-existent	No controls, policies or procedures in place

Key Areas

The CMM focuses on key areas relevant to Information security including:

- Governance
- Risk management
- Compliance
- Incident response
- Access control
- Asset management

Assessment

The CMM involves assessing and evaluating the organisation's processes and capabilities within each key area based on the defined criteria outlined in ISO 27001.

Continual Improvement

The goal of the CMM is to promote continuous improvement in information security capabilities. By identifying current maturity levels and gaps, organisations can develop improvement plans to enhance their security posture over time.