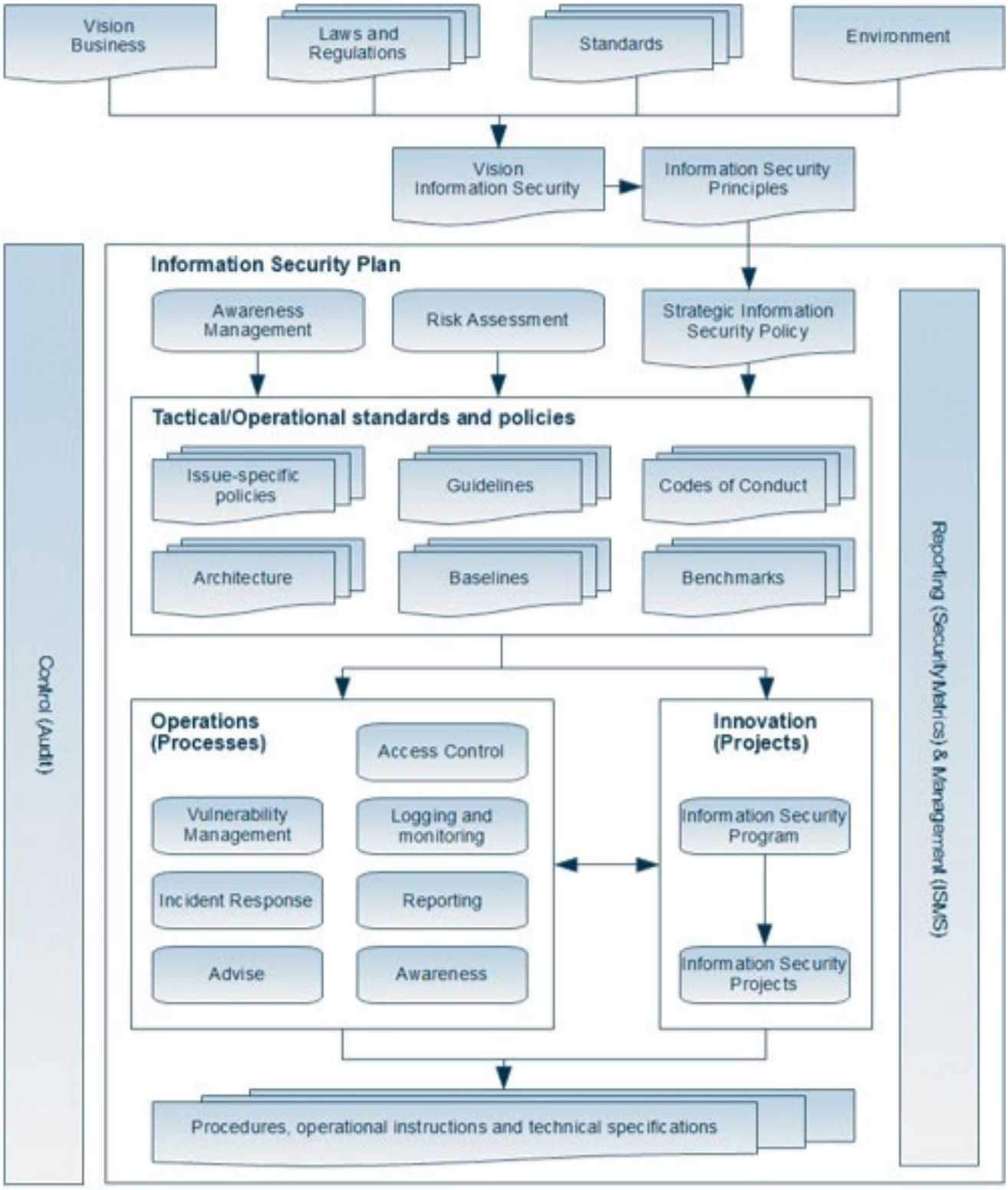
SECO INSTITUTE

Information Security Management Framework (ISMF) Whitepaper



Introduction

Setting up information security in an organisation is a complex matter. The continuous growth of security threats and responses, and the increasing interconnection between information security and other disciplines represent a major challenge for the establishment and maintenance of effective information security.

The SECO-Institute's *Information Security Management Framework* (ISMF) is a pragmatic model designed to assist organisations in aligning information security with corporate goals and interests and embedding it in the organisation's strategic, tactical and operational management. Simply put, the ISMF intends to provide an answer to the most pressing question in information security management: "What are the things to arrange and in what order should they be arranged to ensure effective information security?"

ISMF at the strategic level

Information security should never be looked at as an isolated discipline. Organisations do not just need information security: they need *the* information security that satisfies their specific needs. This can only be achieved by establishing a strong link between information security and the business, aligning information security with the organisation's goals and needs. This strategic alignment is the beating heart of the ISMF.

Strategic alignment means analysing the following four aspects and using the resulting information as input for the design of information security:

1. the organisation's corporate mission and vision
2. the legal and regulatory requirements applicable to the organisation
3. the quality standards the organisation has implemented/is planning to implement
4. the organisation's environment, the socio-political context in which the organisation exists

1. The corporate mission and vision describe the organisation's goals and ambitions, and the policies that will be needed to achieve these goals and ambitions. Understanding corporate goals and ambitions enables security professionals to anticipate technical/ organisational changes and future needs, and determine how these changes and needs can be facilitated or satisfied by information security. Demonstrating that information security is directly connected to corporate goals and needs creates a stronger position for information security in C-level discussions and facilitates gaining support for information security.

2. Laws and regulations impose mandatory requirements on the organisation. Many of the laws and regulations that apply to the organisation (corporate governance, e-commerce and data protection laws, or financial regulations, to name just a few) have important information security implications. The relevant legal and regulatory requirements (and the compliance obligations derived from them) should be identified and incorporated in the information security design to ensure and demonstrate information security's contribution to the organisation's overall compliance efforts.

3. Quality standards are either imposed on the organisation by a regulatory body (for example, in the case of a medical device manufacturer) or implemented by the organisation voluntarily to guarantee the quality of products and services, increase efficiency and productivity, and gain a competitive advantage by enhancing customer trust. Just as laws and regulations, quality standards contain requirements that are highly relevant for the organisation's information security.

4. 'Environment' refers to the organisation's socio-political context, the overall political and social expectations that exist towards the organisation. These expectations play a crucial role in aligning information security with corporate goals and needs. Some organisations, for example, are generally expected to attach more importance to security than others, and therefore also suffer a more significant reputational damage if a security breach occurs. While a small travel agency may survive a security breach without experiencing major consequences, the same breach at a bank would result in a high degree of media attention and a severe impact on consumer trust.

Analysing the above four factors provides us with a long list of "*would-likes*", "*musts*" and "*shoulds*" (desires, obligations and expectations). These elements (and the role information security plays in in achieving or facilitating them) should be included in a **vision on information security.**

The vision on information security outlines how information security can help the organisation to achieve the "*would-likes*" and take care of the "*musts*" and the "*shoulds*". In other words, the vision describes how information security can facilitate corporate goal attainment, how information security can reduce or eliminate obstacles, and how information security can create new opportunities for the organisation to maximise the chances of success. A compelling vision conveys a positive message about information security.

The vision on information security rests on **generic information security principles**. These principles are simple statements that govern decision-making in unprecedented situations and provide a starting point for strategic policies. For example: "*We always opt for the alternative that implies the lowest risk level*" or "*We prefer proven technology and best practices to new technologies and methods*".

In the possession of an elaborate vision on information security and well-formulated generic information security principles, the Information Security Plan is created.

The Information Security Plan (IS plan) is a framework to translate the vision to strategic policy and implementation strategy. Within the IS plan framework, three essential components need to be addressed:

1. Strategic information security policy – Creating a document that outlines, in general terms, what actions the organisation will take in respect of information security. For example: "*All employees will sign a code of conduct*" or "*Everyone must adhere to the clear desk and clear screen policy*".

2. Risk assessment – The identification of the organisation's assets and potential areas of concern provides a good starting point for the strategy.

3. Awareness – Instilling information security awareness in the organisation (including the C-level) is an important prerequisite for truly effective information security.

ISMF at the tactical level

At the tactical level, the instruments necessary to manage operational-level information security are listed and/or created. These instruments include:

Issue-specific information security policies: binding agreements relating to a particular topic, for example access control policies, clear desk/clear screen policies, or mobile device policies.

Guidelines: recommendations with a less binding character than policies.

Behavioural codes: documents setting out rules for the required or desirable behaviour.

Architecture: documentation of how the components should be interconnected to ensure efficiency and goal attainment (risk sharing, interoperability, standardisation and harmonisation).

Baselines: minimum security requirements for (components of) the information systems that must be met under all circumstances. These are usually defined in relation to asset/information classification.

Benchmarks or **secure configuration baselines:** describe how a device should be configured to ensure a certain level of security, for example "*mobile hotspot should be disabled*".

ISMF at the operational level

At the operational level, we can distinguish between two sorts of activities: processes (ongoing activities, such as project management or reporting) and innovations (projects).

For information security, the most important **processes** are **management**, **implementation** and **reporting**. The information security organisation manages, implements or monitors different activities on behalf of the organisation (from intrusion detection systems to information security awareness) and informs the organisation of the state of play in technical and organisational security in different reports.

The implementation of (innovative) **projects** always entails new risks. In order to ensure information security's contribution to corporate goal attainment, information security needs to ensure that the security aspect is integrated in all projects and project management in general.

Another important aspect is to align information security projects with other projects for better resource planning.

At the operational level, the most important documents (**operational arrangements)** are procedures, work instructions and technical documentation.

Procedures are general descriptions of the actions to be taken to ensure and facilitate compliance with the organisation's (more abstract) policies.

Work instructions

Work instructions are detailed documents that describe how the actions (described in procedures) must be performed.

Technical documentation includes information on the organisation's servers, devices, log files, etc.

ISMF reports can be grouped into three categories:

1. **Compliance reports** centre around compliance with laws, regulations and standards. These reports are the auditor's centre of attention.
2. **Security reports** revolve around the organisation's current state of security. These reports are necessary as compliance reports neither reflect nor guarantee the organisation's state of security. Compliance reports are intended for Security Management.
3. **Performance reports** are drawn up to show what benefits information security has delivered for the organisation as a whole and justify the investments made. These reports are aimed at the C-level.

ISMF and audits

Audits can be aimed at testing compliance with laws, regulations and standards (compliance audits) or testing whether the organisation's measures are still sufficient and fit for their purpose. Just as compliance reports, compliance audits do not guarantee a level of security: they only assess whether the requirements are met without looking at qualitative aspects.

ISMF in relation to Information Security Management System (ISMS)

The agreements that result from addressing the above aspects, should be implemented through an Information Security Management System (ISMS), such as the one set out in ISO27001. The ISMS management tool will ensure the effective implementation and control of all agreements through a plan-do-check-act cycle.