Designing an Effective Information Security Policy for Public Organizations:
ISO 27001 as a Success Framework

Yassine Maleh
https://orcid.org/0000-0003-4704-5364
University Sultan Moulay Slimane, Morocco

Mustapha Belaissaoui
https://orcid.org/0000-0003-3877-9235
Hassan 1st University, Morocco & National School of Business and Management in Settat (ENCG), Morocco

INTRODUCTION

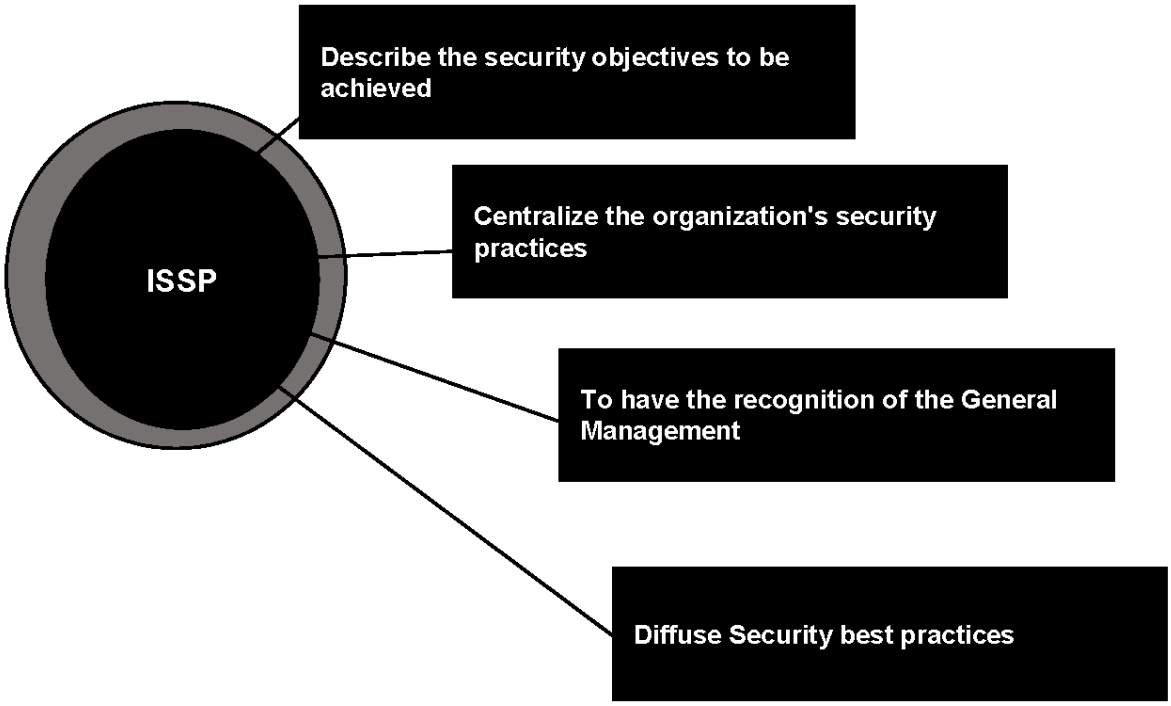
Information Systems (IS) are today an integral part of the functioning of public administrations and bodies, the activity of businesses and the way of life of citizens. The security of these information systems has become a major issue for all public or private sectors, which would be very strongly affected in the event of serious malfunctions (T. R Peltier, 2016).

Information security policy is the general term used to describe any document that transmits an element of the security program in order to ensure compliance with the organization's security goals and objectives. Since this definition covers a wide range of security policy documents, it is useful to describe the various types of information security policies that an organization may use. The terms used below to describe these types of information security policies are generally used in the information security industry and will be used consistently throughout this paper (Ifinedo, 2014). However, it is not unusual for a government organization or agency to have different names for the same types of information security policies. For example, in many organizations and certainly in government departments, the word "policy" is closely associated with laws and regulations (Rees, Bandyopadhyay, & Spafford, 2003). In these cases, a limited number of individuals (e.g., the legislature) have the power to create a policy, so that an information security policy is generally referred to by other names such as "information security statement", or "information security document" or other terms avoiding the use of the word "policy". The term used by an organization to describe these documents is irrelevant. The overall organization and completeness of these documents are important (Hong, Chi, Chao, & Tang, 2006).

The Information Systems Security Policy (ISSP) reflects the expectations and requirements of the Executive Management with regard to the Information System (Canavan, 2003; Höne & Eloff, 2002b) (Canavan, 2003). It must take into account at least the needs in terms of availability, confidentiality and integrity of applications and data used and transiting on networks and systems. It consolidates a set of technical, organizational, legal and human security rules and principles to ensure an efficient and uniform level of security (Fomin, 2008). The ISSP is the counterpart of the Information Systems Master Plan for security. It can lead to an ISSP action plan that prioritizes projects to meet ISSP objectives. The objectives of the Information Systems Security Policy (ISSP) are described in figure 1.

DOI: 10.4018/978-1-7998-3473-1.ch081

Figure 1. Information system security policy objectives



There are several standards and best practice guidelines to assist organizations in implementing an information systems security policy such as ISO 27000, ISACA, NIST, etc. ISO 27001 (ISECT, 2012) is an international standard that is part of the ISO 27000 family of standards (Von Solms, 2005). It refers to a set of standards relating to the information security management system. The ISO 27001 standard is a British standard that came into being in October 2005, succeeding in the BS 7799-2 standard. It describes the requirements for the implementation of an Information Security Management System as shown in figure 1. This standard allows companies to choose security measures to ensure the protection of sensitive assets within a well-defined perimeter by implementing a systematic and proactive approach to security risk management.

Best practice guides such as ISO 27001, COBIT, ISACA do not provide the practical framework for implementing an IS security policy (Höne & Eloff, 2002a). The objective is to guide organizations in their approach to implementing an IS Security Policy through a practical guide to implementing an IS Security Policy.

Problem Statement

Many prescriptive approaches to ISO 27001 already exist, for example, ISO 27003, which is the official standard with guidelines for ISO 27001 (Talib, M. A., El Barachi, M., Khelifi, A., & Ormandjieva, 2012). Several steps to implement the management framework provided in ISO 27001, called information security management system ISMS, are presented. However, a practical methodology for implementing an information security policy does not exist.