Chapter 9
Classifying and Securing Information

ABSTRACT

This chapter focuses on the classification and security stage in the information lifecycle. The chapter identifies the key questions to answer in formulating an information strategy. Concepts associated with these issues and the consequences of ignoring them are explained. The issues are also interpreted in different internal operating environments and in the context of future business environments.

CLASSIFYING AND SECURING INFORMATION IN THE LIFE CYCLE

Security and Classification is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information (Peltier, 2010; Peltier, 2016). The information or data may take any form, e.g. electronic or physical. Information security’s primary focus is to balance potential harm and value. Every organization must determine the types of harm that may result from using or providing access to their organization. Harm must be determined while ensuring that value is realized. Security levels are defined and assigned through a multi-step risk management process that identifies assets, threat sources, vulnerabilities, potential impacts, and possible controls, followed by assessment of the effectiveness of the risk management plan. Security classes assigned to information assets are paired
with user privileges to ensure that assets are available to those who need them, and protected from accidental disclosure or discovery by those who are not permissioned. User privileges are often associated with groups of users, depending on roles and positions within or external to the organization. In some cases, though, security may be associated with a storage system or location, or with individuals. Chapter 9 presents key decision points related to security and classification, including considerations for different business and working environments. Chapter 9 presents key decision points related to securing and classifying information, including considerations for different business and working environments.

KEY QUESTIONS

Chapter 9 provides a deep dive into the key questions and decision points in the secure and classify stage of the life cycle. We offer 24 more specific questions intended to guide your thinking about how to secure and classify information assets and to prevent liabilities. The questions also form the basis of an audit of information assets. An audit should ask and answer all of the questions listed in this chapter. From these answers you should be able to judge the strength or weakness of assets in this stage of their life cycles.

These questions are organized into five easy to remember categories to help you work through them as you work on your strategy. We do not offer answers to these questions because only you can determine which answers best suit your environment. There is no single right or wrong answer. Short explanations are provided for key concepts as background and context. These explanations also serve as a working reference source for both business and information professionals.

The What Questions

Your strategy should explain….

- The organization’s essential definition of harm?
- The circumstances under which information may result in liabilities?
- The harm that may result from the mismanagement of information assets?
Challenges and Solutions for Complex Business Process Management
www.igi-global.com/chapter/challenges-solutions-complex-business-process/36563?camid=4v1a