Available online at www.sciencedirect.com
ScienceDirect
The Journal of Systems and Software 80 (2007) 1590–1593
The Journal of Systems and Software
www.elsevier.com/locate/jss

IT compliance of industrial information systems: Technology management and industrial engineering perspective

Sangkyun Kim *

Department of Industrial Engineering, Kangwon National University, Chunchon, Republic of Korea

Available online 26 January 2007

Abstract

IT compliance is one of the hottest issues in IT and technology management fields. The purpose of this paper is to provide a common framework for IT compliance. First, a review on the compliance age is provided. Second, the characteristics of business records communicated via industrial information systems are described shortly. Finally, an IT compliance framework is suggested. The framework of this paper is not proven by industrial studies because the spread of IT compliance and the industrial response to it are still under progress. Future works should prove the practical value of this framework and should include technical studies.

Keywords: Compliance; Technology management; Industrial information system; Records management

1. Compliance age

According to the definition of standard dictionaries, compliance means cooperation with or obedience to the law. Information Technology (IT) compliance means an accordance of corporate IT systems with predefined policies, procedures, standards, guidelines, specifications, or legislation. Table 1 summarizes some laws which lead to IT compliance requirements.

Since the US securities laws of the early 1930s, the SOA is one of the most well-known legislations on enterprise governance, financial disclosure and the practice of public accounting. The SOA aims to improve corporate accountability to investors and creditors (Burrowes et al., 2004). The rising of the SOA has contributed to an increase of industrial awareness IT compliance (Kim, in press).

The case of Morgan Stanley provides a guide to best practice which shows why a company should take a serious view of IT compliance. According to WS&T Staff (2006), Morgan Stanley failed to submit tens of thousands of e-mail records during a Commission investigation carried out from December 2000 to July 2005. The SEC investigated why Morgan Stanley failed to provide sufficient records according to an anonymous report which insisted that Morgan Stanley had destroyed their e-mail records on purpose. The Securities and Exchange Commission declared that Morgan Stanley did not provide sufficient e-mail records from backup media and most of backup media had been overwritten. Finally, Morgan Stanley was charged with noncompliance with the federal securities laws which require a company to produce, keep, and provide its records. The result of the Morgan Stanley case was that they lost a $15 million civil penalty (Sanchez, 2005). The judge on the Morgan Stanley case left an important precedent of IT compliance which enforces companies to produce and keep e-mail records, and provide them upon government request.

2. Business records in industrial information systems

In industrial information systems, an e-mail, instant messenger (IM) message, DB query, and contents interacted via the world wide web (WWW) are recognized as critical business records which should be secured, monitored, maintained, retrieved and controlled. The lifecycle

* Tel.: +82 33 250 6280; fax: +82 33 255 6281.
E-mail address: saviour@yonsei.ac.kr

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.01.016

Table 1
Legislation on compliance

Legislation	Target	Compliance issues	Penalties
Sarbanes-Oxley Act (SOA) of 2002	All public companies subject to US security laws	Internal controls, records management and financial disclosures	Criminal and civil penalties
Gramm-Leach-Bliley Act of 1999	Financial institutions	Security of customer records	Criminal and civil penalties
Health Insurance Privacy and Accountability Act(HIPAA)	Health plans, health care clearinghouses, and health care providers	Personal health information in electronic form	Civil fines and criminal penalties

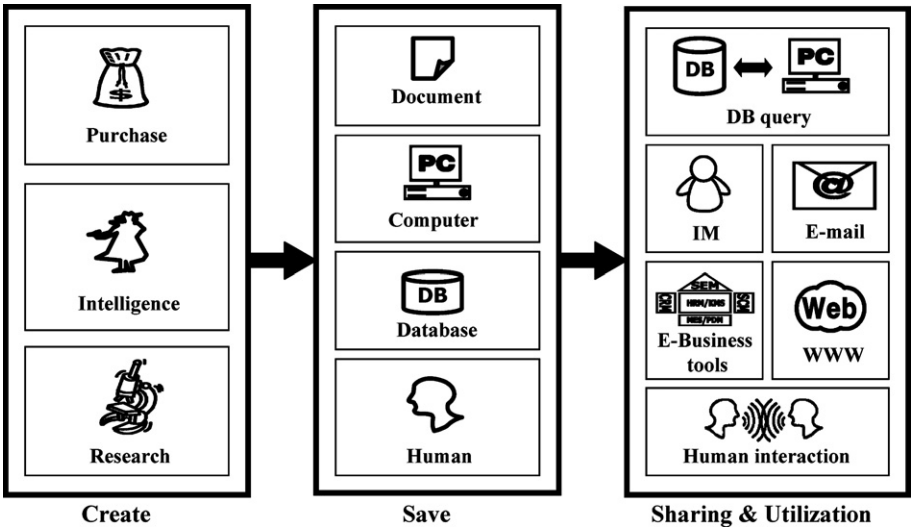

Fig. 1. Lifecycle of business records.

of business records consists of the creation, saving, and sharing and utilization steps as illustrated in Fig. 1. In the first step, business information is created by purchasing, research or intelligence activities. Secondly, created information is memorized by human brains or stored as documents, or in databases or computers. Thirdly, stored or memorized information is shared and utilized via IT methods including DB query, e-mail, IM, WWW, e-business tools, or human interaction.

However, it is very difficult to manage all the business records in a centralized system because of the following factors: e-mail records are stored, accessed and managed by distributed users and their computers (DiCenzo and Couture, 2005); IM provides real-time dialogue and file transfers among multiple users with their own computers who are connected to the Internet. Everyone connected to the Internet can easily use IM by downloading from the Internet or using OS-embedded IM software (Grey, 2001; Kim and Leem, 2005a); Databases are an organized collection of business records that can be accessed via network environments by personal users and they adopt non-standard protocols; The WWW is emerging as the most popular application on the Internet, is used for many diversified business purposes (Cheung, 1998), has the most business potential (Jemmeson, 1997), and exchanges and shares information (Hong, 1999), however it is difficult to control employees use of the WWW based on a corporate policy (Kim and Choi, 2005).

3. IT compliance framework

This chapter provides an IT compliance framework based on the background of technology management, industrial engineering, and information engineering. The IT compliance framework described in this chapter could be applied as the framework of enterprise records management. Table 2 summarizes previous works related with IT compliance frameworks.

Based on the implications of previous works on IT compliance which are described in Table 2, the requirements and architecture of the IT compliance framework are derived as follows:

- *Composition of key components*: Considering previous works on IT control and legal requirements, various security functions should be provided fundamentally. Studies on records management show that various modules which could gather business records from various messaging systems should be provided. Under the requirements described in various legislations, functions for gathered business records and evidence management should be presented. Finally, the approaches on gover-