

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/220422725>

# Information security standards focus on the existence of process, not its content

Article in *Communications of the ACM* · August 2006

DOI: 10.1145/1145287.1145316 · Source: DBLP

---

CITATIONS

69

---

READS

883

1 author:



**Mikko Siponen**

University of Jyväskylä

**119** PUBLICATIONS **3,972** CITATIONS

SEE PROFILE

# Information Security Standards Focus on the Existence of Process, Not Its Content

The existence of prescribed security processes in organizations does not mean the goals of the processes are achieved.

Information security management standards are among the most widely used methods of security management. These standards, BS7799 and its latest version BS ISO/IEC17799:2000 in particular, have been praised as being the keystone in any successful information security management activities [4, 7, 9, 11, 12]. Since information security management standards are widely used and advocated by researchers and practitioners, it is important to note these standards have an important limitation. They focus on ensuring that certain information security processes or activities exist, while they are unconcerned about and fail to give advice on how these security processes can be accomplished in practice. Clearly, it is not important that something is done, but what really matters here is how well it is done. The sidebar describes how this problem pertains to

four prestigious information security management standards: BS ISO/IEC17799:2000, GAISP [5], SSE-CMM (2003), and the Standard of Good Practice for Information Security [8].

## EXAMPLES OF PROCESS ORIENTATION

Information security management standards are primarily concerned with ensuring the existence of processes rather than the content of these processes. Process refers to a set of principles (or security activities), by which systems are rendered secure. For example, “carry out a risk analysis” and “set up an awareness program” are examples of principles that are part of the process. This lack of paying attention to the content problem manifests itself in two ways. First, it means the standards are more concerned with ensuring certain information security activities exist in organizations

and are less interested in how well they are done. Second, these processes, guidelines, and the principles provided by the information security management standards are abstract and simplified, and do not provide advice on how the desired results are to be achieved in practice.

This lack of content problem stems from the fact that the existence of a security process or security activities as such do not say anything about the quality of the process. That is, the fact that an organization has in place a certain security process or security activity prescribed by the information security standards does not imply the ultimate goal of this process (or security activity) is therefore achieved. It does not mean the organization's systems are secured according to this objective. Here, I provide examples from each of the four information security management standards to illustrate this problem. The first

## Merely setting up a training session or presenting information security policies and guidelines will not ensure employees actually follow the information security procedures correctly.

BS ISO/IEC 17799: 2000, p. 11	SSE-CMM, (2003 p. 319).
<b>6.2 User Training</b> To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.  Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.	<b>PA01: Administer Security Controls</b> Goal 1 Security controls are properly configured and used. BP.01.03 Manage security awareness, training, and education programs for all users and administrators.

**Table 1. Information security management standards illustrating the lack of content problem: BS ISO/IEC17799 and SSE-CMM.**

example is from BS ISO/IEC17799: 2000 and the second from SSE-CMM (2003)—see Table 1.

The example from BS ISO/IEC17799: 2000 shown in Table 1 suggests employees should follow security producers correctly, and the standard implies that producing an introduction to information security awareness programs (education and training activities) is the way to ensure this. However, the standard does not suggest how users should be trained or motivated to follow information security procedures (that is, what is the actual content of these information security awareness activities). Clearly, merely setting up a training session or presenting information security policies and guidelines will not ensure employees actually follow or internalize their information security mission [1, 10]

and follow the information security procedures correctly. Indeed, the important contentual question of what constitutes the appropriate behavioral (educational and

The Standard of Good Practice for Information Security	GAISP
<b>Section SM1.2 Security Policy</b> There should be a documented information security policy.....  The information security policy should prohibit: making sexual, racist or religious statements, which may be offensive...	<b>2.1.3. Ethics Principle</b> ([5], p. 13) Information should be used, and the administration of information security should be executed, in an ethical manner. <i>Rationale:</i> Information systems pervade our societies and cultures...use of information and information systems should match the expectations established by social norms, and obligations.
	<b>2.2.14 Equity Principle (GAISP p. 16) Ethical Practices</b> ([6], p. 49) Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.

**Table 2. Information security management standards illustrating the lack of content problem: The Standard of Good Practice for Information Security [8] and GAISP [5]; GASSP [6] and GAISP ([5], Version 3.0) principles.**

motivational) strategies to be used in such information security education and training is not addressed. Extracts from the SSE-

CMM (2003) indicate similar problems (see Table 1). SSE-CMM prescribes information security awareness programs for all employees, while it does not say anything regarding how this is done in practice—what education strategies should be followed within such programs.

The stress on the existence of certain information security process or activities, without paying attention to the content, may incline us to the view that the

information security management standards only naively list obvious things. One may argue that we all know that employees should follow information security procedures, and this is not the problem. The real problem is how you actually ensure people do in fact follow the security procedures. The next example, from the Stan-

## FOUR INFLUENTIAL SECURITY MANAGEMENT STANDARDS

### Generally Accepted Information Security Principles (GAISP)


The development of GAISP, formerly known as GASSP [6], began in 1992 with support from the U.S government, the International Information Security Foundation, and several organizations around the world ([6], p. 28). Version 2.0 was published in 1999, while in version 3.0 the name was changed to Generally Accepted Information Security Principles (GAISP). As the name indicates, GAISP aims to document the accepted security principles and practices [5]. See [www.issa.org/gaisp/gaisp.html](http://www.issa.org/gaisp/gaisp.html) for further information.

### BS ISO/IEC17799

BS7799 is the most well-known and respected standard measured by the number of articles devoted to it (see [11]). Its latest version—BS ISO/IEC17799: 2000—has been accepted as an ISO standard. BS ISO/IEC17799 is intended for use in securing organizations' information systems. In addition, organizations complying with BS ISO/IEC17799 may apply for certification, which attests to their compliance with this standard.

### System Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM version 3.0 (2003), coordinated by the International Systems Security Engineering Association (ISSEA), is designed to be used for certifying the maturity level of an organization's information systems security and improving the security processes of organizations. By reference to a maturity level, organizations can demonstrate to their customers and business partners that they are trustworthy organizations. SSE-CMM offers five information security maturity levels on a scale of 1 (poor) to 5 (high) for this purpose. For more information, see [www.sse-cmm.org/lib/lib.asp](http://www.sse-cmm.org/lib/lib.asp).

**The Standard of Good Practice for Information Security** (2003 version) has been developed by the Information Security Forum (ISF), an international association, and is supported by more than 250 organizations worldwide. The standard aims to provide the international, authoritative, and comprehensive benchmark for information systems security. The standard is updated every two years; see [www.isfsecurity-standard.com/index\\_ie.htm](http://www.isfsecurity-standard.com/index_ie.htm) for more details. 

dard of Good Practice for Information Security [8], illustrates this situation.

One may claim it is self-evident that there should be “a documented information security policy...” and the policy should not

make racist statements (see Table 2). The more crucial issue, not addressed by The Standard of Good Practice for Information Security, is how information security policy is made in practice: how do practitioners know when

a security policy is good? For example, since organizations are different, they have different business and security requirements. Then how are information security policies developed individually for each organization to pay attention to an organization's unique requirements?

Table 2 presents the “ethical practices” principle of GASSP [6, p. 49], later termed as “Equity principle” in GAISP [5]. It is admirable that GASSP/GAISP tries to address ethical aspects. But again it is important—and even perhaps self-evident—that information security activities must be able to withstand moral scrutiny. However, recognizing this, the problem remains that it is anything but easy to say what an “ethical manner” means (see Table 2). GAISP does not offer practitioners much definitive help in this respect. It only suggests the relativistic position that what is morally right and wrong can be determined by exploring social norms. However, GAISP does not reveal how you actually do this. Nevertheless, it is highly questionable that what is morally right and wrong can be determined on the basis of “established social norms,” as suggested by GAISP. It is easy to imagine several cases where the following of what is socially acceptable behavior in a culture may intuitively be seen as problematic. Hackers are known to form their own hacker culture with its particular social norms (hacker ethics). Even if hackers

would be seen as the norm of “social behavior” in hacker culture, it does not lead to the conclusion that hacking is therefore morally right.

To give another example, software piracy is a socially accepted activity in many countries. Thus, according to GAISP, the copying of software would be morally acceptable in these countries. Moreover, organizations in the Internet era must do business with other countries and cultures whose cultural norms differ. Thus, what is morally right and wrong cannot be derived per se from “social norms,” as the philosopher David Hume first recognized. The fact that someone is engaged in an action does not tell us anything about the morality of that action.

GAISP’s statement that we should respect “the rights and dignity of individuals” (see Table 2) is a good example of the problems discussed. Again, it does not state what the rights of individuals are. Yet, given that we have some rights, how far do others need to go in respecting our rights (must they sacrifice their own rights)? For example, given that the individual has a right to privacy, in what cases can one violate these rights? GAISP bypasses this important issue, namely, how you actually decide what is morally right (when you violate individuals’ privacy).

## **FUTURE STANDARDS AND RESEARCH SHOULD PAY ATTENTION TO CONTENT**

The preceding examples from the four information security man-

agement standards illustrate the problem of focusing on information security process, while failing to consider the content of this process: how well the security activities are carried out, and how exactly the objectives are to be achieved in organizations.

Practitioners should be aware of this problem, and acknowledge that paying attention only to the existence of certain information security actions prescribed by information security management standards, and not their content, may provide a false sense of security. Future or updated information security management standards should pay particular attention to this problem. It is the contents—and its quality—that really matters.

Researchers can also help. Instead of listing rather obvious things (for example, have a security policy) or high-level security goals (users should comply with security policy and guidelines), practitioners would benefit from in-depth experiences and lessons learned from the use and application of information security management standards in organizations. Through case or action research, researchers could obtain such information on how the objectives of security standards are attempted to be met in organizations where information security management standards are applied. Even better, scholars can participate and use their knowledge in efforts applying the information security management standards in organizations. ■

## **REFERENCES**

1. Abrahamsson, P. The role of commitment in software process improvement. Ph.D. thesis. *Acta Universitatis Ouluensis A 386*, Oulu University Press, 2002.
2. *Code of Practice for Information Security Management, BS7799-1*, Department of Trade and Industry, British Standard Institution, London, U.K., 2000.
3. *Code of Practice for Information Security Management, BS7799*, Department of Trade and Industry, British Standard Institution, London, U.K., 1993.
4. Eloff, M.M. and Solms, S.H. Information security management: A hierarchical framework for various approaches. *Computers and Security* 19, (2000), 243–256.
5. Generally Accepted Information Security Principles (GAISP) Version 3.0, 2003; [www.issa.org/gaisp/\\_pdfs/v30.pdf](http://www.issa.org/gaisp/_pdfs/v30.pdf).
6. Generally Accepted System Security Principles (GASSP). Version 2.0. *Information Systems Security* 8, 3 (June 1999).
7. Hardy, G. Standards—The need for a common framework. *Computers and Security* 14, 5 (1995), 426–427.
8. ISF Standard of Good Practice for Information Security (2003); [www.isfsecuritystandard.com/index\\_ie.htm](http://www.isfsecuritystandard.com/index_ie.htm).
9. Janczewski, L. Managing security functions using security standards. In L. Janczewski, Ed. *Internet and Intranet Security Management: Risks and Solutions*, Idea Group Publishing, 2000, 81–105.
10. Siponen, M.T. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security* 8 (2000), 31–41.
11. Solms, R. Information security management (3): The Code of Practice for Information Security Management (BS 7799). *Information Management and Computer Security* 6, 5 (1998), 224–225.
12. Solms, R. Information security management: Why standards are important. *Information Management and Computer Security* 7, 1 (1999), 50–58.

---

**MIKKO SIPONEN** (Mikko.T.Siponen@oulu.fi) is a professor the Department of Information Processing Science at the University of Oulu, Finland.

---