Information security policy – what do international information security standards say?

Karin Höne[2] and J.H.P. Eloff[1]

Department of Computer Science
Rand Afrikaans University
E-mail:[1]eloff@rkw.rau.ac.za
[2]KarinH@gensec.com

Abstract

One of the most important information security controls, is the information security policy. This vital direction-giving document is, however, not always easy to develop and the authors thereof battle with questions such as what constitutes a policy. This results in the policy authors turning to existing sources for guidance. One of these sources is the various international information security standards. These standards are a good starting point for determining what the information security policy should consist of, but should not be relied upon exclusively for guidance. Firstly, they are not comprehensive in their coverage and furthermore, tending to rather address the processes needed for successfully implementing the information security policy. It is far more important the information security policy must fit in with the organisation's culture and must therefore be developed with this in mind.

Keywords

information security policy, international standards, information security, elements, characteristics

1. Introduction

There are various controls and measures that can be – and indeed need to be – implemented within an organisation to ensure the effective working of information security. These controls and measures range from technical solutions and contractual regulations to organisational awareness of current risks, threats and vulnerabilities. Undoubtedly, the singularly most important of these controls is the information security policy.

The information security policy is a direction-giving document for information security within an organisation. It is a document that indicates management's commitment to and support of information security, as well as defining the role information security has to play in reaching and supporting the organisation's vision and mission [JISC01]. In essence, the information security policy is documented to explain the need for information security – and its concepts – to all of the organisation's information resource users. It should complement the organisation's business objectives and reflect management's willingness to operate the organisation in a controlled and secure manner.

Although the information security policy is a vital part of an organisation's strategy for achieving information security, it is not always easy to put this document together. There are often differing opinions within the organisation as to what constitutes a policy. Questions are asked as to what should be incorporated into the document, what it should look like, how long it should be, who needs to approve it, and many more. Generally, the authors of this important document just want to know: "How do we go about documenting an effective information security policy for our organisation?" Because of the difficulties experienced in developing such a policy, the elected authors often turn to other organisations' policies, commercially available sources or templates available from public sources, such as the Internet, for answers to their questions. This is also often done to compensate for a lack of skills and

0167-4048/02US$22.00

understanding needed for writing an effective information security policy. Such an exercise then generally results in a "cut and paste" effort that does not truly reflect the culture of the organisation and thus does not result in an effective direction-giving document for information security within the organisation.

This article attempts to find answers to the above questions, as well as to the dilemma of what should be used as a starting point in developing an information security policy. This is done by investigating what various international information security standards have to offer in terms of guidance and requirements for writing an effective information security policy. Through the industry experience of the article's authors and the research of various publications related to developing an information security policy, a list of elements commonly included in such a document was identified. These elements include topics such as the roles and responsibilities of the users regarding information security in an organisation and management's commitment statement towards information security. A second list, describing the general characteristics of an information security policy, such as the length of the document and review period, was also drawn up. Each item in these lists is briefly introduced below, and then they are used in an evaluation exercise to determine the usefulness and applicability of the international standards in developing an information security policy.

2. Elements of an Information Security Policy

The elements of an information security policy focus on the different parts that make up such a document. The elements focus mainly on the overall content of the policy.

Need for and Scope of Information Security

This is a brief introductory statement emphasising the organisation's dependence on information and therefore information security [OOIT01]. This introductory statement also provides the background as to why the policy is needed in the organisation.

Objectives of Information Security

The objectives of information security in an organisation should be described briefly to inform the reader of the specific aim of information security management in the organisation. These objectives should be clearly linked to the organisation's overall business strategy, goals and objectives and the nature of its business [OOIT01].

Definition of Information Security

An information security policy is generally targeted at a diverse audience for whom information security may be a foreign and new concept. It is therefore crucial that the policy contains a brief and understandable definition of information security to ensure a uniform understanding of the concept throughout the organisation.

Management Commitment to Information Security

The commitment statement is the singularly most important statement in an information security policy. Without this statement, any activities attempted by the information security personnel will not be effective and will not be taken seriously throughout the entire organisation [JISC01]. The management commitment statement can force employees to pay attention to information security and demonstrates management's intention of making a success of it in the organisation [WOOD95].

Approval of the Information Security Policy (Signature)

The approval signature can also be seen as the endorsing signature and should typically be that of the highest possible signatory in the organisation [OOIT01]. This signature should

be displayed in a prominent position as a further sign of top management's commitment to information security.

Purpose or Objective of the Information Security Policy

The purpose or objective of the information security policy should not be confused with the introductory statements on the need for information security in an organisation. These statements rather describe the reasons for the development of an information security policy and will possibly be linked to legal compliance issues. The main goals of the policy itself are thus described in this section [JISC01].

Information Security Principles

The information security principles describe the general rules related to information security within an organisation. These principles try to explain to the users what is the correct and the incorrect behaviour in the organisation regarding various topics and concepts. Some of these principles will be closely linked to an organisation's culture or to regulatory requirements governing the industry in which the organisation is functioning. Others will, however, be applicable to all organisations and will be found in any information security policy, such as virus protection and user awareness and education. The principles will, however, also change over time depending on technological developments and changes. An information security policy written 20 years ago will generally make no reference to any form of electronic information security, but will probably make detailed reference to physical information security. It is therefore crucial that especially this part of the policy be regularly reviewed for applicability.

Roles and Responsibilities

This is one of the most important components of the information security policy, as this part tells the reader exactly what is expected of him/her in terms of information security in the organisation. The roles and responsibilities should cover all aspects of information security, as well as the individual responsibilities of all parties using the organisation's information resources [OOIT01].

Information Security Policy Violations and Disciplinary Action

The statement on information security policy violations is a very powerful statement, as it ensures that disciplinary action can be taken against a user if the policy is not adhered to. It is very important that this statement be directly related to the organisation's overall disciplinary policy.

Monitoring and Review

This statement deals with the need to frequently monitor and review the continued applicability and effectiveness of the information security controls implemented within the organisation [BSI00]. Without this statement there is no forced continuity for the improvement of information security implementation in the organisation.

User Declaration and Acknowledgement

This is not a common element found in an information security policy, and is usually presented as an appendix or a separate document. It is, however, a very useful element, as it is typically drafted as an abridged version of the information security policy and targeted completely at the users of the organisation. The users are then more likely to read the entire section and have a better understanding of what is expected from them. In signing a user declaration upon employment before access to electronic information is granted, the user acknowledges his/her responsibility with regard to information security. The user declaration and acknowledgement should also be read and signed again on an annual basis by all users to remind them of their individual responsibilities in protecting information assets within the organisation [TUDO01].

Cross References

The information security policy should never be written in isolation and will need to be supported by other relevant policies, standards, procedures and processes. These applicable documents should be referenced in the policy to ensure that the reader obtains a complete picture of all information security controls and measures used in the organisation. Often organisations are also required to implement certain controls and measures as determined by the country's legislation and regulations. These then also need to be referenced in the policy.

General Elements

Below is a brief list of further recommended elements to be included in an Information Security Policy to ensure its official status in an organisation. These elements are self-explanatory and will only be listed below.

- The authors
- Date of the policy
- Review date of the policy

3. General Characteristics of an Information Security Policy

The general characteristics of an information security policy describe the way in which such a document should be written.

The policy should be short and easy to read. Various lengths ranging from between one and five pages are recommended. It is important to remember that if the policy is too long, the users of the organisation will not read it.

The writing style of the policy should reflect the organisational culture to ensure acceptance of the document by the organisation's users. Various terminologies are unique to specific business environments and should be considered and remembered when writing the policy. This implies that a policy written for a manufacturing plant will not necessarily be understood equally well in a financial services environment. The policy should be clear and comprehensible to all users in the organisation and also avoid the use of technology terms to the extent possible.

Of great importance is also the visual impact the policy has on the users. A document accompanied by a clever script or visual interpretation of the policy will have a much greater impact on the user community than just a couple of pages filled with text. These considerations are essential during the dissemination and distribution of the policy.

An information security policy should be reviewed periodically to ensure that it remains current, as well as relevant to the information security objectives of the organisation. It is also important for the information security policy owner to remember to review the document after major changes in the technological environment and regulatory requirements to determine whether the document still applies. Avoiding the references to particular technologies would, however, ensure that the document does not have to change too often or too rapidly, thereby creating a comfort zone of familiarity for the users.

It is essential that the policy remains clear and comprehensive, but above all it must be realistic. The policy must be practically implementable and enforceable and, most importantly, distributed and communicated throughout the organisation to every user of the organisation's information assets. The policy can be distributed in numerous creative ways and once again these should be linked to the organisation's traditionally effective communication channels. These channels may include e-mails, a web presence or even workshop-type sessions where the document is explained to the users.

4. International Information Security Standards

The international information security standards recognise that the information

security policy is an important topic and therefore it is generally covered early on in the different standard documents. The extent to which the policy as a topic is covered in these documents, however, differs vastly, with some of them spending only one or two short paragraphs on the topic, and others providing concise point-by-point guidance.

All the international standards researched are available in the public domain in various formats. Below is a brief description of each of the researched standards, as well as an indication of how the topic of the information security policy is addressed in each.

BS7799

BS7799 is a United Kingdom standard covering the management of information security. Its stated objective is:

> to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used. [BSI99]

Part 1 of BS7799 (Code of Practice for Information Security Management) has recently been adopted as an ISO standard, i.e. ISO/IEC 17799. The standard has furthermore been used in various countries as the basis of regional information security-related standards, e.g. Australia and New Zealand.

BS7799 and its variants give a brief point-by-point description of what should be included as a minimum in an information security policy. This standard goes on to explain what should be done with the policy in the organisation, i.e. that it should be approved by management, published and communicated throughout the organisation. BS7799 also includes a section exclusively on the review and evaluation of an information security policy.

BSI IT Baseline Protection Manual

The IT Baseline Protection Manual from the German Bundesamt für Sicherheit in der Informationstechnik (BSI) presents a set of recommended standard security controls, or "safeguards" as referenced in the manual. The published goal of the BSI manual is:

> to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and can also serve as the basis for IT systems and application requiring a high degree of protection. [BSI00]

The BSI document gives a comprehensive description of drawing up an information security policy, covering topics such as the responsibility of management regarding the policy, convening a team responsible for the development of the policy and the content and distribution of the policy. The section on the content of the policy gives guidance on the minimum information to be included, as well as brief pointers on the style and review of the document.

COBIT

The Information Systems Audit and Control Association & Foundation (ISACAF) developed COBIT to provide management and business process owners with an IT governance model to help understand and manage the risks associated with IT. The stated mission of COBIT is:

> to research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors. [ISAC00]

COBIT describes the processes and controls needed for implementing an information security policy, rather than focusing on the document itself. It does contain a brief section on the Security and Internal Control Framework Policy, which gives various pointers on writing and maintaining such a document.

Generally Accepted System Security Principles (GASSP)

GASSP is a set of generally accepted system security principles based on recommendations of a report "Computers at Risk", published by

the United States of America's National Research Council [I²SF99]. This document therefore has a strong US-centric and governmental flavour. Of all the standards researched, this is the least-known document and has the smallest distribution.

GASSP's reference to the information security policy is minimal and focuses on the rationale for such a policy, as well as the different processes needed for defining, maintaining and implementing the policy. The concept of a policy hierarchy is furthermore explored in depth.

GMITS (ISO/IEC PDTR 13335-1)

The Guidelines for the Management of IT Security (GMITS) are produced by an ISO Joint Technical Committee. The intended purpose of the guidelines is to provide comprehensive guidance on information security with regard to its planning, management and implementation [ISO01].

GMITS first describes the policy hierarchy recommended for organisations before giving a point-by-point listing of what topics an information security policy should at least cover.

ISF's Standard of Good Practice

Recently made available to the public domain, this document from the globally representative Information Security Forum (ISF) aims to provide an achievable target for organisations against which they can measure their performance regarding information security management. It examines information security from a business perspective and focuses on how organisations can keep the business risk associated with critical information systems under an organisation's control in today's ever-changing technological world [ISF00].

The ISF document contains a brief point-by-point section on the information security policy. It focuses very much on acceptable user behaviour, as well as the characteristics of the policy.

5. Evaluation of International Information Security Standards

Each of the international information security standards described above were measured against the list of elements and general characteristics of an information security policy to determine its coverage in the various standards. The table below gives an indication of which elements and characteristics were indeed covered in the standards (indicated by the X marks in the various columns). It should, however, be noted that the table does not give any indication of the extent of the coverage, i.e. whether the elements or characteristics are simply mentioned or whether they are in fact explained in detail.

As can be seen from the evaluation table overleaf, the international standards do not cover all the elements and characteristics to a great extent. Most of the standards agree on the importance of explaining the need for and scope of information security, as well as the inclusion of a management commitment statement. Furthermore, all of the standards agree that the definition of roles and responsibilities should be included in an information security policy. Bringing attention to violations of the policy, as well as the related disciplinary action, is also important.

However, few of the standards attempt to define the actual information security principles to be included in the policy, i.e. the individual topics that should be covered by the document. This may be attributed mainly to the fact that an information security policy should have a longer-term lifespan, whereas new concepts and technologies are developed much faster. The international standards, of course, also ideally have a lifespan that may outlive some of the technological and other concepts relevant today. Furthermore, the

Elements and Characteristics	BS7799	BSI	COBIT	GASSP	GMITS	ISF's Standard of Good Practice
Need for and Scope of Information Security	X	X	X	X		X
Objectives of Information Security	X	X				
Definition of Information Security	X					
Management Commitment to Information Security	X	X		X		X
Approval of the Information Security Policy (Signature)						
Purpose or Objective of the Information Security Policy						
Information Security Principles:	X	X				X
- Legal, regulatory and contractual compliance	X				X	X
- User awareness and education	X	X			X	
- Virus prevention and detection	X					
- Business continuity planning	X				X	
- System development and procurement					X	
- Risk management					X	X
- Personnel issues					X	X
- Outsourcing management					X	
- Incident handling					X	
- Information classification		X				X
- Access Control		X				
Roles and Responsibilities	X	X	X	X	X	X
Information Security Policy Violations and Disciplinary Action	X	X	X		X	X
Monitoring and Review		X				
User Declaration and Acknowledgement						
Cross References	X					
General Elements:						
- The authors						
- Date of the policy						
- Review date of the policy						
Length		X				
Style		X				
Format	X	X				X
Review	X	X				X
Distribution	X	X				X

international standards attempt to transcend international boundaries and are therefore conscious of cultural and regional issues and try to avoid these.

There are various other elements and characteristics found in the different research resources that are not mentioned in any of the international standards. The ultimate reason for this may in fact be that international standards often deal with processes rather than being prescriptive regarding the content of documents.

All of the international standards have something of value to offer to as a starting point for an information security policy. Of greatest benefit would be to have access to more than one of these international standards to ensure that the broadest possible range of elements and

characteristics is researched. Keep in mind, however, that an international standard will not write the document for you, i.e. the actual wording needed for an organisation's information security policy has to come from the organisation itself – the organisational culture.

Conclusion

The information security policy is one of the most important documents in an organisation and must therefore be written with due care. It is not an easy document to write and therefore most authors of such a document look for as much help as possible in writing it. The first points of reference when attempting an information security policy are often the international standards on information security. These standards, however, are not comprehensive in their discussions of the information security policy, with some of them covering the topic in one or two short paragraphs only. These standards attempt to describe the various processes and controls needed for successfully implementing an information security policy, rather than advising what the policy should look like.

Yes, the international standards on information security go a fair way in answering the questions posed at the beginning of this article. It is, however, crucial to the effectiveness and success of an information security policy that the answers to these questions come from within the organisation. This ensures that the policy is seen as the organisation's own and goes a long way in the users' committing and adhering to it.

References

[BOWD01] Bowden, Joel S. 14 August 2001. Security Policy: *What it is and Why – The Basics.* http://www.sans.org/infosecFAQ/policy/sec_policy.htm

[BSI00] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2000. *IT Baseline Protection Manual.* http://www.bsi.bund.de/gshb/english/menue.htm

[BSI99] British Standards Institute (BSI). 1999. BS7799 *Code of Practice for Information Security Management.*

[DTI00] Department of Trade and Industry (DTI). 2000. *The Business Manager's Guide to Information Security.* http://www.dti.gov.uk/

[HELW00] Helwig, Steven M. 15 December 2000. *Security Policy for Higher Educational Institutions.* http://www.sans.org/infosecFAQ/policy/higher_edu.htm

[I²SF99] International Information Security Foundation (I²SF). June 1999. *GASSP (Generally Accepted System Security Principles).* Version 2. http://web.mit.edu/security/www/gassp1/html

[ISAC00] Information Security, Audit and Control Association (ISACA). July 2000. *COBIT 3rd Edition Control Objectives.* http://www.isaca.org

[ISF00] Information Security Forum (ISF). November 2000. *The Forum's Standard of Good Practice.* http://www.isfsecuritystandard.com

[ISO01] ISO/IEC JTC 1/SC 27. October 2001. PDTR 13335-1 *Information Technology – Security Techniques – Guidelines for the Management of IT Security (GMITS) – Part 1: Concepts and Models for Managing and Planning IT Security.*

[JISC01] Joint Information Systems Committee (JISC). 16 March 2001. *Developing an Information Security Policy.* http://www.jisc.ac.uk/pub01/security_policy.html

[OOIT01] Office of Information Technology. January 2001. *Information Security Guidelines for NSW Government Agencies (Part 1 – Information Security Risk Management).* http://www.oit.nsw.gov.au/Guidelines/Security_Part1.pdf

[OSBO98] Osborne, Keith. 1998. Auditing the IT Security Function. *Computers & Security,* 17 (1), pp. 34 – 41.

[TUDO01] Tudor, Jan Killmeyer. 2001. *Information Security Architecture: An Integrated Approach to Security in the Organization.* CRC Press LLC. ISBN 0-8493-9988-2.

[WOOD95] Wood, Charles Cresson. 1995. Writing InfoSec Policies. *Computers & Security,* 14 (8), p 667 – 674.