

Certifying an Organization's ISMS

By Fiona Pattinson CISSP, CSDP and Willibert Fabritius CQM

This article contains a brief discussion of the role of an information security management system (ISMS).

A management system describes the people, processes and technologies used to focus and manage the activities of an organization. Each organization builds a unique system that is supportive of the goals of that organization. The system will reflect different disciplines depending on the values and culture of the organization. So, we see systems defined with very different areas of focus such as enterprise management, environment, health, safety, quality, web content, personnel, risk and many other topics; and with different emphasis on security factors such as the well-known triad of confidentiality, integrity, availability, or on topics such as privacy or product assurance.

Even though each organization builds a unique system, the management systems have several common elements, and are based around an improvement cycle. One most often used is based on W. Edwards Deming's famous Plan Do Check Act (PDCA) cycle. This cycle guides us as we plan the action of what needs to be done and how best to go about it, establish the controls that we need, monitor progression, and improve the system—taking preventive and corrective actions and identifying areas for improvement. Study of management systems has shown that there are several common elements including policy, planning, implementation and operation, performance assessment, improvement, and management review.

An information security management system (ISMS) is focused on managing information security within an organization, a topic that is of growing concern to many organizations as they deal with the challenges presented in the information society including evolving information security and privacy legislation (see the table below), published guidelines (OECD, Cyber security), and threats natural (fire, flood, earthquake, tornados) or human introduced (viruses, SPAM, privacy, hacking, industrial espionage).

In an ISMS the information protected includes not just that residing in electronic format on computer or network, but includes paper-based information and extends as far as intellectual property. A properly implemented ISMS can be effectively used by either small or large organizations, and can be tailored to support the protection of information in diverse organizations including data processing centers, software development, e-commerce, health care organizations, finance, manufacturing, service organizations, non-governmental organizations, colleges, and not-for-profit organizations.

So, how does an ISMS support information security? Effective implementation of the framework ensures that a management team, committed to information security, provides appropriate resources to support the processes that the organization needs to achieve appropriate information

security. It needs to be emphasized that this commitment of senior management is absolutely crucial in the success of this—and other—management systems. This inevitably includes processes related to the basic management of the system, and training and awareness. It emphasizes a risk management process that guides the choice of safeguards and that, coupled with the metrics necessary to ensure that the chosen controls are implemented correctly, ensures that the system evolves to manage the changing business and security environment, and that the resulting management system is, and continues to be, effective.

Companies operating across several jurisdictions have the added challenge of ensuring that the various legislations and regulations are identified and compliance ensured.

The Benefits of Using an ISMS

By using an ISMS an organization can be sure that they are measuring and managing their information security processes in a structured manner and that they can control and hone their system to meet their business needs. If they draw from a standardized ISMS framework they can be sure that they are drawing from the experience of many others and that the system has been reviewed and reflects best practices. Such a framework is a tried and tested tool that helps management ensure that security-resource is spent on the most effective areas for the business. Is the money available to spend on information security better spent on a firewall and network security technology, or would investing in training personnel bring more effective results?

In the U.S. the Sarbanes Oxley Act of 2002 requires that adequate internal controls are in place for information security. Implementing an effective ISMS is the best way of meeting that requirement.

BS 7799-2:2002 is aligned with the popular ISO 9001:2000 quality management system, ISO 14001:1996 Environmental Management system or even ISO 18001:1999 Occupational, Safety and Health management system (which means that they all can be, and usually are, easily integrated). It is applicable to both large and small organizations and thanks to its popularity, is a de-facto internationally recognized standard.

A Brief History of BS 7799, and the Growth of Their Use Internationally

BS 7799-1, the "Code of Practice for Information Security Management" began life as a British standard. First published in 1995, it contained best practice security controls to support industry and government organizations in the implementation and improvement of information security. Once it was published, organizations recognized the value in a common framework and its popularity grew. In 1998 BS

7799-1 was revised, taking into account identified improvements and updates, and adding new controls in consideration of the developing technologies in the field such as e-commerce, mobile computing and third party activities.

The international interest in the code of practice (part 1) led to its submission as the basis for an ISO standard. Subsequently ISO/IEC 17799 was published as an international standard in December of 2000. ISO/IEC 17799 is now maintained within the remit of Working Group 1 of the information security committee ISO/IEC JTC1 SC27 "IT Security Techniques". It is impossible to know the number of organizations using ISO/IEC 17799 today, but it is the most popular security standard in terms of sales, and is referenced not just by BS 7799-2 but by a host of other frameworks and guidelines.

Shortly after the development of BS 7799-1 in 1995, the need to define the management system to host the controls in the "Code of Practice" was identified and BS 7799-2: "Specifications for Information Security Management Systems" was developed to address that need. In order to align BS 7799-2 with the quality management system standard ISO 9001:2000 it was revised and was re-published in 2002.

Other countries published their own national standards substantially based on BS 7799 including the Netherlands (SPE20003), Australia/New Zealand (AS/NZS 4444), Denmark and Sweden (SS627799), and India (IS 14357:2002). BS 7799 was also translated into many different languages, and it can now be obtained in Chinese (Mandarin), Danish, Dutch, Finnish, French, German, Japanese, Korean, Norwegian, Portuguese, and Swedish.

BS 7799-2 continues to grow in popularity, with over 700 organizations registered as compliant with the standard in June of 2004. (An international register is maintained by the ISMS International User Group and is available at <http://www.xisec.com>)

The Structure of the Standards

First it is important to realize that BS 7799-2 is deliberately defined to be very general. It is meant to be applicable to, and provide consistency between, disparate organizations. This fact leads us to underline that the scope of the management system is very important. The organization in question can be a multi-national corporation through to a small project team, a small business, or even a non-commercial organization.

The definition of the ISMS itself is given by BS 7799:2002-2 (or its national equivalents). Defining the fundamental best practices of the management system, this standard ensures that a risk assessment is made, and that this is used to correctly select the safeguards from the code of practice given in ISO/IEC 17799:2000. A "statement of applicability" documents the applicable safeguards and is a flexible document, depending on the vulnerabilities and threats that have been identified for the organization in question. The statement of applicability will change to meet the challenges presented by new and evolving risks; it may not use all the controls documented in the code of practice, and it can even give rise to new ones that aren't in the ISO/IEC 17799 standard.

A process-based approach is followed, allowing the organization the flexibility of operating the processes that are appropriate to it. These include understanding the business information security requirements, establishing appropriate policies and objectives, implementing and managing (through meaningful measurements) the appropriate safeguards, monitoring and reviewing the performance and effectiveness of the ISMS itself, and ensuring that the system continually improves.

Diagram of PDCA in BS 7799 (See Figure 1).

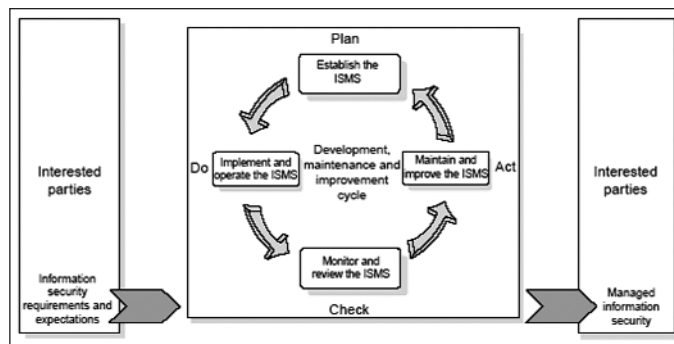


Figure 1: PDCA model applied to ISMS (From BS7799-2:2002)

When implemented, the system is expected to draw from sources appropriate to the scope of the management system. These sources are likely to reflect parameters such as the size, focus, values, and geographical positioning of the organization. For example, a software development organization may reference processes drawn from a software development agile methodology, or a capability maturity model; whereas a data processing center may consult a technical report such as ISO/IEC TR 13335 (Guidelines for the Management of IT Security). Those providing information services may follow BS 15000:2002 IT service management.

Specialist ISMS exist: For example in the U.S. NIST continue to develop an ISMS system in response to the U.S. Federal Information System Management Act of 2002 which includes standards and guides which provide a complete ISMS that is mandatory for U.S. Federal systems. The NIST guidelines and standards are an excellent resource for non-federal systems and may be implemented by commercial organizations under the BS 7799-2 umbrella. These include risk management (SP 800-30), categorization of information and information systems (SP 800-60), security planning (SP 800-18), security control selection and implementation (SP 800-53) and verification of security control effectiveness (SP 800-53A). The framework includes guidance for the Security Certification and Accreditation of Federal Information Systems (SP 800-37).

ISO/IEC 17799:2000 contains safeguards, or controls, addressing several risk areas relevant to information security. It is not appropriate to describe them in detail here, but by looking at the various high-level paragraphs of the standard the breadth of activities can begin to be appreciated. Inevitably this code of practice cannot address every situation, and the standard allows further controls to be specified when needed. The control areas include:

- ▲ Security Policy
- ▲ Organizational Security
- ▲ Asset Classification and Control
- ▲ Personnel Security
- ▲ Physical and Environmental Security
- ▲ Communications and Operations Management
- ▲ Access Control
- ▲ Systems Development and Maintenance
- ▲ Business Continuity Management
- ▲ Compliance

The Certification Process, What Assurance an Organization or Third Party Can Draw From it?

It is worth re-stating that the certification scheme in use does not allow for certification of compliance with the code of practice ISO/IEC 17799. No formal scheme exists to assess compliance with ISO/IEC 17799:2000.

What is assessed is that the information security management system meets the requirements of the management system standard (BS 7799-2 or one of the standards adopted nationally that is based upon it).

In order to ensure meaningful and repeatable assessments against the standard it is necessary to use an independent and accredited third party known as a "certifying body". An accreditation body is responsible for ensuring that the certification bodies reach the necessary standards for consistently assessing that an ISMS implementation is meeting the BS 7799-2 standard. There are several accreditation bodies including UKAS (UK Accreditation Service) and DAR (Deutsche Accredierungs Rat—German accreditation association) who operate under agreement with the International Accreditation Forum (IAF), and follow the European EA-7 /01 standard. Operating under the auspices of the Japanese government is JIPDEC (Japanese Information Processing Development Corporation)

While accredited under an approved scheme the certifying body is able to certify that your organization meets the standard, and will register compliant management systems with the accreditation body. This is not the end of the story. It is necessary not only that you reach the standard, but also that you maintain and improve the standard. Your certifying body needs to ensure that you do, so surveillance audits will be scheduled to ensure that you continue to meet the requirements of the standard, and that it is maintained to meet the needs of the organization.

Similarly, the auditors who are tasked with assessing the implementation of an organization's ISMS need to meet common standards to ensure that results are measured accurately and are repeatable. To support this, auditors are trained and maintain their professional status under a similar scheme of accreditation. An example of which is that offered by the International Register of Accredited Auditors (IRCA).

Caveat emptor! When an organization is claiming certification check that:

- ▲ They are claiming certification to BS 7799-2, not ISO/IEC 17799! Only the former gives you any assurance of the effectiveness of the ISMS. There is no scheme for certifying ISO/IEC 17799.
- ▲ The certifying body is accredited to perform the assessment.
- ▲ The scope of the certification is appropriate. Like ISO 9001 the assessment of the system hinges around the scope of the management system. This might be very broad—include an entire international company, or it might be defined to include one site, a functional area, even one team.

Apart from the benefits of implementing and using an ISMS that were discussed above there are several additional benefits to having it certified to meet best practices. These are often intangible and may be divided into two major groups: internal and external benefits.

The internal benefits include:

- ▲ Senior management gets an independent review and report of the strength and weakness of the organization's ISMS.
- ▲ An often ignored benefit is the simple fact that people have the tendency to follow rules and regulations if they believe that they could/will be audited.
- ▲ In some cases certification is a contractual requirement between and organization and its customer.

The external benefits include:

- ▲ The organization demonstrates to interested parties (stakeholders) its commitment to adhere to established guidelines.

- ▲ Customers and other stakeholders develop trust in the certification body. This adds value to the organization that has had its ISMS certified. It can also lead to tangible benefits in the reduction in the number of audits performed by suppliers and other second parties.
- ▲ The perception by stakeholders that an organization that is willing to voluntarily submit to an external examination is open and willing to learn.
- ▲ The reputation of an organization can be of vital importance to an organization working in the information fields. Just one published security incident can destroy years of work and significantly affect the good-will value. More tangibly, research is beginning to show that the value of a company can be affected by just such an incident.
- ▲ If your organization's sector is one in which information security is valued, then a certified ISMS can offer a differentiator between you and your competitors. "Would you rather do business with a company that has an accredited third party's assurance that the management system for information security is good, or one that doesn't?"
- ▲ Certification by an accredited certification body may offer you a defense should you ever be subjected to litigation in relation to information security related legislation. If you can prove that you follow industry best practices then perhaps you may make the case that you had taken reasonable precautions.

The Basic Steps of Certification

1. Ensure Senior Management commitment. This is vital to success, and should be considered throughout the process.
2. Define and implement the system. Make sure that you think very carefully and understand the ramifications of your chosen scope. There are several guidelines and consultants who can help you achieve this.
3. Ensure that the system is operational and has been through at least one cycle of improvement. (This includes internal audits.) It is important to notice that there are at least two levels where improvement can, and should occur: the technical level and the system level.
4. Identify a certification body, and arrange for the certification audits. The selection should be passed on criteria like expertise of the used auditors as well as the reputation of the certification body.
5. Optionally have a pre-assessment of the system to identify any likely areas of non-conformance. This is also an excellent opportunity to get internal auditors acquainted with the thinking process of third party auditors. Ensure Senior Management commitment.
6. Usually, a "desktop audit" is performed, which includes the examination of your documentation and records.
7. A full on-site audit of the ISMS is being performed.
8. If non-conformances are made then these need to be addressed appropriately. Ensure Senior Management commitment.
9. Hang the certificate on the wall!
10. Be ready for surveillance audits designed to ensure that you are maintaining and improving on the standard that you reached initially.

Common pitfalls.

The typical pitfalls in implementing an ISMS are related to:

- ▲ **Lack of Senior Management's commitment**


- ▲ **Scope issues:** insufficient, inaccurate, or even plain wrong
- ▲ **Awareness of employees:** many organizations face the challenge of ensuring that ALL employees are aware of the applicable policies—activating screensavers, firewalls, virus detection systems just to name a few.
- ▲ **Expertise of employees:** also can be described as competence of employees. The real problem is not only on the expert level but also on management and user levels. Technology changes with an ever increasing speed is partially the reason for this, but also the lack of training on ALL levels. Organizations are simply not providing sufficient training to their employees.
- ▲ **Implementation flaws:** open firewalls, routers with default passwords, deactivated security measures. These flaws are quite often the result of lack in awareness or expertise of employees.
- ▲ **No risk assessment:** resulting in spending resources in areas that are important, but ignoring those areas that are MORE important.
- ▲ **Insufficient resources:** organizations are constantly in the process of resource allocation; the challenge is for many organizations the proper/correct allocation of resources—many ISMS suffer in this area as management fails to conduct an adequate risk assessment.
- ▲ **Inadequate, insufficient asset classification:** Many organizations are lacking the clear, concise classification of information (e.g. public, internal use only, confidential, secret, top secret). This leads to inconsistency in the implementation.

An Indication of the Future of the Standards

The power and effectiveness of an ISMS based on a process approach has been tried and tested by BS 7799-2. Its growing popularity, and the ISO management system paradigm, have attracted much attention and demonstrate the need for an internationally recognized scheme. This has been recognized by ISO, which has performed the preparatory groundwork

and begun the process for developing an internationally recognized ISMS standard. ISO 17799 is already a long way through its first scheduled revision, and a new version will be published in due course.

Conclusion

Ensure Senior Management commitment. Organizations which have not started a formally implemented Information Management system should use BS7799 and ISO/IEC 17799 as a guideline to implement such a system. Those organizations that are conscientious about their reputation with stakeholders and/or need a differentiation among their competitors need to consider third party certification of their ISMS. 

Fiona Pattinson is a management consultant specializing in quality and information-security processes. She serves on the INCITS T4 committee "Security Techniques" which develops the US position on standards within the remit of ISO SC27, and is Co-Chair of the US Chapter of the Information Security Management Systems, International User Group. (www.us-isms.org).

Willibert Fabritius is a Certified Lead Assessor performing ISO 9001, QS-9000 & TS 16949 as well as BS7799 audits. He is also a Certified Quality Manager with some eleven years experience in implementing quality management systems. Mr Fabritius holds a masters degree in Computer Science from the University of Aachen (Germany). He is a member of the American Society for Quality. For the last nine years he has been employed by TUV Rheinland Inc as a Lead Assessor and has gained a vast experience in the implementation of quality management system.

We would also like to acknowledge the support we received from Dr. Alicia Clay of NIST and Ted Humphreys of Xisec.

¹ In his book "Out of the Crisis" Dr. Deming attributes the PDCA cycle to Walter Shewart.