An Introduction to Information Security and ISO27001

A Pocket Guide

by Steve G Watkins

IT Governance Publishing

This page intentionally left blank

An Introduction to Information Security and ISO27001
A Pocket Guide

This page intentionally left blank

An Introduction to Information Security and ISO27001

A Pocket Guide

STEVE G WATKINS

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EH
United Kingdom

www.itgovernance.co.uk

First published in the United Kingdom in 2008
by IT Governance Publishing

ISBN 978-1-905356-69-0

ABOUT THE AUTHOR

Steve G Watkins: Director, Training and Consultancy, IT Governance Ltd.

Steve managed the world's first successful BS7799 implementation project. He has over 18 years' experience of managing integrated management systems, including maintenance of Information Security, Quality, Environmental and Investor in People certifications.

Steve's experience includes senior management positions in both the public and private sectors, having responsibility for nearly all corporate support functions.

As well as being a trained ISO27001 and ISO9001 auditor, Steve is a trained EFQM assessor and holds diplomas in safety and financial management. He is Chair of the UK ISO/IEC 27001 Users Group (which is the UK chapter of the International ISMS User Group) and also sits on the Management Committee of the British Standards Society, where he chairs the Corporate Governance Special Interest Group.

Steve can be contacted at:

swatkins@itgovernance.co.uk.

CONTENTS

INTRODUCTION

This book is intended to meet the needs of two groups:

1. Individual readers who have turned to it as an introduction to a topic that they know little about.
2. Organisations implementing, or considering implementing, some sort of information security management regime, particularly if using ISO/IEC 27001:2005, who wish to raise awareness.

In either case the book furnishes readers with an understanding of the basics of information security, including:

- A definition of what information security means.
- How managing information security can be achieved using an approach recognised worldwide.
- The sorts of factors that need to be considered in an information security regime, including how the perimeters of such a scheme can be properly defined.
- How an information security management system can ensure it is maximising the effect of any budget it has.
- What sort of things resources might be invested in to deliver a consistent level of assurance.
- How organisations can demonstrate the degree of assurance they offer with regard to

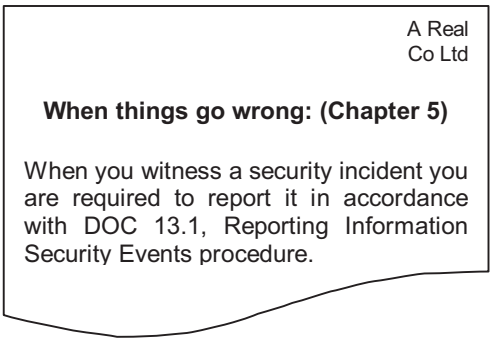
information security, how to interpret claims of adherence to the ISO27001 standard and exactly what it means.

Corporate bodies will find this book useful at a number of stages in any information security project, including:

- At the decision-making stage, to ensure that those committing to an information security project do so from a truly informed position.
- At project initiation stage, as an introduction to information security for the project board, project team members and those on the periphery of the project.
- As part of an ongoing awareness campaign, being made available to all staff[1] and to new starters as part of their introduction to the company.

Corporate users may find they get the most benefit by making the Pocket Guide available and adding a small flyer inside the book which explains how various sections relate to their own specific environment, or where the issues raised in this book are addressed in their own information security management system (ISMS). For example:

[1] Why not conduct sample surveys of people's understanding of some aspects of information security and compile the results both before and after the start of your awareness campaign to demonstrate the effectiveness of your communications and use the figures as one of your 'measures of effectiveness' for management review? See ISO27001:2005 sections 4.2.3.c and 7.2.f.



The book is designed to be read without having to break frequently from the text, but there is a list of abbreviations along with terms and definitions in *Chapter 7* for easy reference. Where footnotes have been added they are not essential reading, and it is recommended you ignore these on your first read through if you are new to the subject – on a second reading they will be of more relevance, and particularly if you are involved in an information security project or decision at any stage.

A word of warning: this is not an implementation or 'How to do it' guide.

Implementing an ISO27001-compliant ISMS requires more advice than a pocket guide such as this could possibly offer. The project is in most cases likely to equate to a significant business-change project, and will require all the project governance arrangements that suit such an undertaking.

There are books available which offer suitably detailed advice, such as *IT Governance: A Manager's Guide to Data Security and ISO27001/ ISO27002* (4th edition) and they can be obtained along with numerous other helpful advice, tools and other related information from the sources signposted in *Chapter 7*.

CHAPTER 1: INFORMATION SECURITY – WHAT'S THAT?

To develop an understanding of what information security means, let's consider something that we all understand the value of: money.

Considering the various aspects of how you look after and use your money, the following emerge as valuable and worthy of note:

Aspect One

You do not want other people spending your money, or at least anyone not given your permission to spend it. This means limiting access to your money, or, when considering information instead of money, keeping it confidential.

This makes good sense, and at first pass may seem to be the only thing that matters. However, if restricting access to your money is all that matters you could have it stored in a totally sealed iron box. Not very useful when you come to want to spend it yourself! This brings us on to our second aspect:

Aspect Two

You want to be able to spend your money when you want to. This means you value the availability of it. Not only this, but you need it to be available in a usable format, so if you

are abroad you want the money to be in the correct currency when you come to spend it.

This also makes good sense. We have identified that in controlling our money we need to consider both restricting access to it (an appropriate degree of confidentiality) and ensuring this is balanced with a suitable degree of availability. However, there is another value that we should be concerned with, and to explain this we might consider the issue of foreign currency a bit more.

Aspect Three

When collecting your currency you do not, at least when first visiting a part of the world that is new to you, know what the money should look like or how you can be assured it is not fake. Most people are content to rely on the reputation of whatever company they choose to exchange their cash with. Nonetheless we do value the fact that what we are being provided with is the real thing and not counterfeit. This is to say that we value the integrity of what we receive.

So with money we value keeping it out of the hands of others, having it accessible when we want it and in the format that we want it in, and that it is what it appears to be.

When referring to information this is the equivalent of valuing the information's confidentiality, availability and integrity; hence when managing the security of information we need to consider these three aspects – much more

than the layman's understanding of the word 'security'!

Organisations that wish to manage their information security arrangements typically introduce a set of policies and procedures that help them exercise a degree of control to provide assurance with regard to these three aspects. This is generically described as an information security management system (ISMS).

Who does it matter to?

Given the definition of information security as the confidentiality, integrity and availability of information,[2] it is relatively easy to determine why this might be of importance to individuals, companies and public bodies.

It soon becomes obvious that it is not just the information that we need to be concerned with, but the storage, handling, moving and processing of it. When considering all of these arrangements it is relatively easy to conclude that every organisation should be concerned with their information security arrangements.

Individuals (members of the public or customers and staff) will want to know that information held about them is being managed and protected appropriately. Theft or fraud involving credit cards, credit ratings and people's very identities

[2] ISO/IEC 27001:2005 defines information security as the 'preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved'.

are well-publicised issues that mean information security is worthy of attention.

Companies will be driven by at least two factors: the requirements of their stakeholders and/or customers, and the need to remain competitive. Public-sector organisations have similar drivers to maintain a strong security stance and safeguard against security incidents.

In fact, many sectors have regulators that demand some suitable form of information management to be in place for anyone offering related services. Various governance regimes include requirements for information and information-processing arrangements, demanding that there are controls in place to enable directors to discharge their duties effectively. With high-profile governance failures in the headlines this is an area where pressure to comply will only grow.[3]

With the increasing trend towards relying on business partners for key services and processes, the need for some form of information security assurance is growing rapidly. Outsourcing and other contracts are now increasingly specifying compliance with some form of information governance regime as a mandatory requirement.[4]

The other key driver is the need to maintain a competitive edge. The obvious aims of not informing competitors of your costs, customers or

[3] See *IT Governance: Guidelines for Directors* by Alan Calder for further information, available through www.itgovernance.co.uk.

[4] More on what assurances such schemes provide and on how to interpret any claims is provided in *Chapter 6*.

trade secrets are concerns that fall within the remit of information security management, as are the less obvious benefits of effective information security such as improvements in customer service through appropriately managed databases (e.g. no longer sending mail shots to addresses that the client has told you they have moved from).

An effective information security management regime can provide an organisation with the foundations on which to build a knowledge management strategy and realise the true value of all the information that it holds.

The public sector has its own drivers, of course, including issues such as justice and national security, as well as the responsibility to become as effective and efficient as possible in conducting its work, in order to be able to truly demonstrate appropriate stewardship of public funds.

To all this is should be added the obvious requirement that staff from any organisation will expect their personal information to be managed appropriately.

CHAPTER 2: IT'S NOT IT

The key message in this chapter is that an effective ISMS needs to address issues relating to personnel, facilities, suppliers and cultural issues, in addition to the obvious area of information technology, and so information security is a topic that goes well beyond the remit of the IT department.

Having identified what information security is, and recognising it as something worth being concerned about, the next stage is to determine exactly what areas and aspects of the organisation will be affected.

Starting with the source of the challenge, we need to include everything that can affect our information, which means including all the equipment on which that information is held, how it is moved/transmitted and any aspects of the business that can affect the information, equipment and related processes. This means we need to set both physical and logical perimeters for our ISMS.

In practice this means that it is necessary to consider the dependencies and interfaces of all aspects of the management system and the information it controls. For example, if we consider information that is sent by courier to another office of the same organisation then we need to include the selection of the courier company and the security requirements placed on the courier through the contract.

With regard to confidentiality it is necessary to consider everyone who has access to the information and the equipment on which it is stored. This is likely to include cleaners and maintenance staff, in addition to directly employed staff.

The system also needs to address the management of information in different formats, including electronic form and hardcopy records. With information in transit, whether it be in the form of papers being taken home for reviewing the night prior to a meeting, or records being sent to archive, it becomes obvious that hardcopy records warrant a similar degree of protection to electronic copies. If a trade secret is accessed by a competitor it does not matter whether it is in an e-mail attachment or on a printed piece of paper – the information that was meant to be kept confidential is out and so any value attached to maintaining its confidentiality is compromised. The value of information is in its content, not in the format it is stored or available in.

Considering these issues, one way or another the ISMS needs to define how it addresses relationships with suppliers, business partners, customers and staff. Of course, the facilities and equipment used to protect and provide information are of equal importance, and also need to be considered within the scope of the ISMS.

In defining the remit of the ISMS this way the organisation is stating the scope of the assurance the system provides. Given the personnel, facilities, suppliers and cultural issues that need to be considered and addressed within the system, it

is obviously a topic that goes well beyond the remit of the IT department.

CHAPTER 3: ISO27001 AND THE MANAGEMENT SYSTEM REQUIREMENTS

As with most topics, there are international standards that deal with information security management, and the main one is ISO27001: 2005.[5]

This standard defines a project approach to aid the design and implementation of an ISMS, and uses the well-recognised Plan–Do–Check–Act model (P-D-C-A) to structure the tasks required to introduce an effective ISMS.

The P-D-C-A cycle can be summarised as:

- Plan what you need to do to achieve the objective (which includes defining what that objective is).
- Do what you planned.
- Check that what you have done achieves what you had planned for it to achieve and identify any gaps or shortfalls (i.e. check whether you have met the objectives).
- Act on the findings of the plan phase to address the gaps and/or improve the efficiency and effectiveness of what you have in place.

[5] Other standards that have been used in referencing information security management over a number of years include BS7799 and ISO17799, but ISO27001 is now the standard for the specification of an information security management system. ISO27002 provides guidance on the implementation of information security.

Typically this last stage will involve making a plan, doing what that plan entails, checking that the objectives were achieved and identifying any shortfalls and then acting on the findings by once again creating a plan.

And so with the introduction of an ISMS using P-D-C-A, the initial cycle of continuous improvement is effected.

One common misunderstanding is that the planning stage is limited purely to planning the project. As far as ISO27001 is concerned the planning stage includes all the work required to determine what is required of the ISMS, and how this is to be achieved. This is a significant undertaking, to the extent that it can take up to half of the project time from initiation through to having a full ISMS in place. The other main resource-demanding stage is implementation. The next chapter deals with the most resource-intensive aspects of the Plan stage.

There are a number of requirements for a management system to operate that are as applicable to an ISMS as to any other management system, and these include:

- **Document control.** This is an arrangement to manage the availability of documents within the ISMS, typically including:
    - the corporate-level policy
    - operating procedures which describe the processes that support the policy and explain who does what, where and when

- work instructions that detail how certain tasks should be conducted, and
- forms which capture the information that is essential for the purposes of review and as evidence of what has occurred.

The aim of the document-control procedure is to ensure that all these documents have been written and approved by the right people and that only the latest approved versions are available to those who need to be aware of and follow them.

- **Control of records.** As important as document control is, it is also important to safeguard records once they have been generated. This means protecting their confidentiality, integrity and availability in order to be sure they can be retrieved by the right (authorised) people when needed and that they are legible and have not been interfered with.
- **Internal audit.** Internal audits can be used for many purposes, but one of the main objectives of deploying an internal-audit regime is to monitor compliance between the management system requirements and working practice. The internal audits are commissioned by the organisation, for the organisation, and provide an opportunity to review the level of compliance within the ISMS by examining what actually happens across a sample of events and processes and comparing this to what the documented management system describes. The identification of any mismatch during an audit provides the opportunity to put

it right, either by changing the system description of what happens, or by enhancing working practices. The internal-audit process should also inform the continual improvement of the ISMS; however, this typically only starts to become an objective of audits once the ISMS is embedded. Internal audits can also be used to investigate specific areas of concern or for the purpose of identifying opportunities for improvement.

- **Management review.** Given that management initiate the ISMS by approving the use of resources to undertake the project and issuing the corporate information security policy defining the objectives of the ISMS, it is reasonable to expect them to review the progress of the implementation project and the effectiveness of the ISMS thereafter. The management review is typically held once every six or 12 months and is intended to achieve exactly these objectives. Typically a number of reports would be prepared for the meeting, covering key indicators of how the ISMS is operating. These reports include an analysis of the outcome of audits (internal and second- and third-party[6]), significant security-related incidents, some form of indicator of awareness of information security issues and the ISMS across all those affected by it, and an indication of the amount and timeliness of any improvement work undertaken. The review

[6] See *Chapter 6* for further information on second- and third-party audits.

should also examine any 'measures of effectiveness'[7] that have been developed.

[7] ISO27001:2005 requires the organisation to define how the effectiveness of security controls will be measured (section 4.2.2.d) and for the management to consider them (section 7.2.f).

CHAPTER 4: INFORMATION ASSETS AND THE INFORMATION SECURITY RISK ASSESSMENT

An asset-based information security risk assessment is the key to any ISO27001 ISMS, forming the lion's share of the Plan phase of the initial P-D-C-A cycle for implementation.

To undertake the risk assessment it is necessary to have defined the scope of the ISMS, and of course to have understood the concept of information security assets: it is the assets that are the subject of the risk assessment.

For the risk assessment to be effective a comprehensive information-asset register needs to be produced. That is to say, a list of everything that has value to the organisation, including information, information processing and storage equipment (every server, computer, laptop, PDA, mobile phone), systems, staff, buildings, etc. This list goes well beyond the more common fixed-asset register.

Each item, or group of items,[8] on this list needs to be risk-assessed using a common methodology.

The value of each asset is estimated for the three information security attributes: confidentiality, integrity and availability. The value assigned to

[8] The grouping of assets for the purpose of risk assessment is more complex than can be covered in this pocket guide. See *Information Security Risk Management for ISO 27001 / ISO 17799* by Alan Calder and Steve G Watkins for more information.

each reflects the total cost to the organisation if that attribute were compromised for the asset concerned, from the cost of replacement, through the consequences for the process(es) it is involved in, to the impact on the organisation's reputation. This is normally best estimated by those involved in the relevant business processes.[9]

These values provide the impact aspect of the classic

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

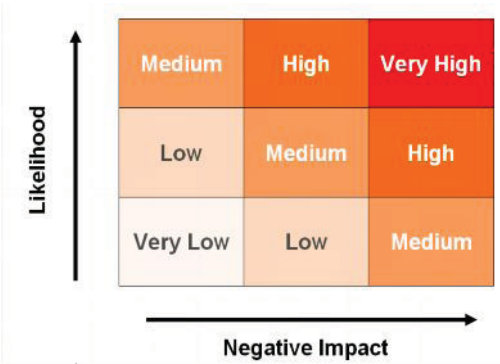
relationship.

The likelihood value comes from the possibility of a threat exploiting a weakness or exposure, or, in information security terms, a vulnerability.

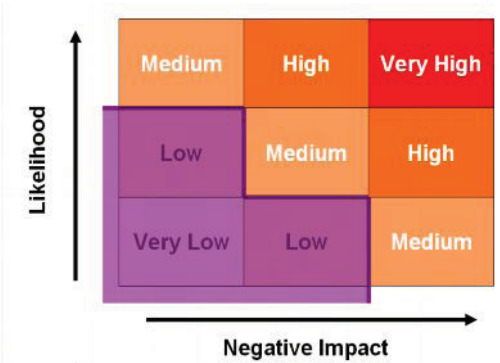
For this to be undertaken against the values associated with the three attributes for all the assets on the register once again requires a common methodology and access to a comprehensive list of threats.

The risk assessment then uses these estimates to determine the risk value for each asset. The relationship between likelihood, impact and risk is demonstrated in the following diagram, in this case showing three levels of likelihood and three levels of impact, which together give five levels of risk varying from 'very low' through to 'very high':

[9] The standard uses the term 'asset owner' in the sense that the owner has control over how the asset is used and controlled. It does not mean they have legal ownership of the asset.



The main aim of an ISMS is to manage all risks to a consistent level of control, and so this is where management need to determine what level of risk is acceptable. For example, they may, using the parameters in the diagram above, decide that risks up to and including 'low' are acceptable, and that therefore it is only those risks that have been assessed as falling above that level of risk acceptance criteria that need managing. In terms of the diagram, the risk acceptance level can be demonstrated by the shaded area as shown here:



Each organisation will have a different level of risk acceptance and this will relate to the organisation's risk appetite – the degree of risk that the organisation is happy to live with on a day-to-day basis.

Risks assessed as falling above the acceptable level are considered and a decision taken as to what to do about each of them. This decision determines which one or more of the following options to apply to address the identified risk:

1. Apply controls to reduce the risk.
2. Accept the risk; this is normally determined by the risk acceptance criteria, but can occasionally be applied even if the risk level is above the acceptable level.
3. Avoid the risk by identifying a work-around that negates the risk.
4. Transfer the business risk to an insurer or supplier.

As different decisions and controls are selected for application to various risks the risk assessment is re-estimated and this process continues until all the assessed risks are estimated to fall within the risk acceptance criteria. The controls are normally taken from the list in ISO27001 at Annex A.[10]

To effect the required level of assurance against information security risks the ISMS needs to ensure that the controls selected through the risk assessment process are in place and applied to the appropriate assets effectively. By informing the selection of information security controls with the risk assessment approach an organisation can ensure that it is maximising the effectiveness of its information security spend, and not leaving any one area of risk open to exploitation at the cost of an inconsistently high level of control elsewhere.

ISO27001 requires a document to be produced that details which controls are applied within the ISMS and which are not. This is known as the statement of applicability.

The whole risk assessment process requires a degree of central coordination, and often benefits from the use of a suitable software solution that can automate many of the potentially resource-intensive administration aspects of the process. The investment in such software really pays back when the ISMS gets into continuous improvement,

[10] The standard helpfully suggests controls are selected from other sources as well, just in case Annex A does not offer sufficient controls to keep pace with the rapidly evolving environment in which we manage security.

as the risk assessment needs to be revisited frequently, either in part or as a whole.

CHAPTER 5: INFORMATION SECURITY CONTROLS

Having now gained an appreciation of the methodical approach to the selection of information security controls and other ways of addressing risks it is time to examine the security controls defined in the international ISMS standards.

The standards themselves go to great pains to emphasise that the controls they detail are not exhaustive, and that each organisation should review them and add their own as required. Typically this would only come about in the early days of an ISMS if there were specific contract or sector requirements that went beyond what is already available. Occasionally there will be technological developments that introduce risks which are not covered to a suitable extent by the existing controls, and so it may be necessary to adopt additional controls.

In the standards there are over 130 controls split into 11 categories, but for the purpose of familiarisation here we are considering them in six groups, and not in any detail. The six groups are not themselves significant and they could easily be formed differently.

Organisation, structure and human resources

This list includes the main controls off which the rest of the system hangs. There is a need for a corporate-level information security policy, which is a statement of the organisation's commitment and objectives relating to information security.

This needs to be available to everyone affected by it, which (as described earlier) includes suppliers, business partners, customers and staff.

There is a need to define where responsibilities for information security lie within the organisation and for the required forums and review bodies to be in place to meet the needs of the ISMS.

The human resources required to undertake all tasks relating to and affecting information security need to be sourced and managed appropriately. This includes considering the sourcing, vetting, management and exiting arrangements for staff, contractors and any other people who interact with the scope of the ISMS, including anyone who has physical access to any premises at or from which information-related assets can be accessed.

Assets, classification and access control

The requirement to maintain a current asset register dovetails with the risk assessment process described in *Chapter 4*. The register needs to go beyond the classic fixed-asset register and include information assets.

There is a control suggesting that assets are classified to a defined labelling scheme, and the classification will indicate the level of protection required and who has approved access rights to them. Access control is also related to ensuring that only those with approved access to the assets can actually access them, and this is subject to both logical and physical barriers.

Passwords and user IT accounts are typical logical access controls, and are of course only as robust as

the practices that manage them. Eradicating poor practices such as writing passwords down, or using sequences or easily guessable combinations, should be strongly discouraged.

Where access issues are risk assessed as requiring a greater degree of assurance, say with regard to accessing a system or application remotely, there is the possibility of two-factor authentication. This is where each unique user has to deploy in combination both a physical key (token) and a logical key (password) to be granted access. An example here is a credit card being swiped in a store (the magnetic strip or smart chip being the physical key) and your personal identification number (PIN – the logical key). Of course, when using a credit card online the physical aspect normally disappears if you have sufficient details to hand in another format, and hence the request for further numbers which are normally sourced from the card, or passwords separate from your PIN. Some banks are addressing this weakness by issuing card readers to account holders and asking that they use these for some sites and particularly for online banking.

There are also controls which can be deployed, such as session timeouts, that require the user to re-enter selected logon criteria every so often and duress alarms that consist of a predetermined series of apparently innocuous key strokes which alert network or system monitors to a problem without making anyone in the vicinity of the user aware that an alarm has been activated.

Physical access

Physical access is, of course, a concern for information security. Anyone who has access to the equipment or medium on which information is stored could potentially walk out with that asset and the information assets stored on it. Whilst some protection can be offered to prevent access to information stolen in this manner, it will still affect the availability of that information and possibly the resulting integrity of the data asset as well. With continuing advances in technology it is impossible to remain ahead of thieves and crackers or hackers. Passwords can often be broken and whilst encryption (the use of pairs of numeric algorithms, or keys, one to scramble information and its counterpart to unscramble it) provides an enhanced level of unwanted access prevention (logical, not physical), there are incidents of encryption controls being beaten, almost exclusively due to the mismanagement of keys, and so the combination of logical and physical controls is essential to an efficient, effective ISMS. Perimeters around secure areas should be defined in all three dimensions – tunnelling in through the floor, or using an air vent in the ceiling, may still allow enough access and egress for theft to take place.

Networks and IT

The largest category of controls relates to IT operations and network management. They cover issues including planning and testing new developments prior to implementation, capacity planning for all aspects of the network and systems, segregation, network design and technical

vulnerability management. Issues such as back-up are mentioned here, along with testing of the back-up so that, as an example, any accidentally deleted filed can be restored from the copy of all files (the back-up) run the previous night.

When things go wrong

There are a number of categories which deal with the handling of problems, events and/or incidents.[11] These are additional to the improvement-process requirements of maintaining an ISMS, and deal with what should be done in reaction to, and in order to recover from, a security breach.

The severity of information security breaches can vary massively. If the problem is likely to cause a significant challenge to the normal running of operations it is desirable for some form of business continuity to be invoked. This area of control includes the need to regularly test the business continuity plans (BCPs) in order to learn from the experience and improve the plans ahead of their being called upon for real.

Of course, not all security incidents require such a dramatic response, but the degree of reaction and the method for determining escalation should be defined.

[11] ISO27001 defines information security incidents and information security events separately. Not all events are, or will be, incidents, but both require management and this should be defined. Clarification should also be given as to when an event might escalate to incident level or be classified as such.

All of these issues are key areas for information security awareness campaigns, as the organisation should be in a position to benefit from notification of a potential problem as soon as possible. This therefore means that awareness needs to be raised and maintained for all relevant parties, including suppliers, business partners, customers and staff. Often cleaners will be among the first people at a site each day, or the last to leave it, and they should be trained and required by contract to report any security-related observations to an appropriate contact.

Compliance and internal audit

These categories are relatively self-explanatory: they deal with legal and technical compliance. The organisation should be aware of, and comply with, its legal obligations. Technical testing should report on the degree to which IT equipment, systems and software are as they should be. The schedule can include checks to confirm that only the right, approved equipment is connected to the network, that systems and software are as required (the approved mix and number for the licences held), and can include penetration testing to confirm the resilience of the technical measures in place.

CHAPTER 6: CERTIFICATION

As with many other management system standards, there is a scheme that can be used by organisations to demonstrate their compliance with the internationally recognised standard for information security management, ISO27001.

Companies wishing to use this standard to demonstrate the robustness of their information security management arrangements need to subject themselves to an external audit.

For the assurance provided by the outcome of the audit to be recognised, the audit needs to be conducted in compliance with the recognised scheme; that is, the 'accredited certification scheme'. This is is administered by the United Kingdom Accreditation Service (UKAS) in the UK and certificates issued under this scheme will bear the UKAS logo:

The audits are conducted by accredited bodies; those seeking to demonstrate compliance with the standard become certificated, not accredited.

Accreditation bodies around the world sign up to a memorandum of understanding that results in mutual recognition of each other's schemes – so a certificate issued by the Joint Accreditation System of Australia and New Zealand (JAS-ANZ) will be the equivalent of one issued by UKAS – hence a worldwide scheme exists.[12]

The scheme enables organisations to demonstrate a degree of assurance with regard to their information security practices. The integrity of this scheme means that customers can rely on certification rather than insist on sending their own auditors in to provide the assurances required by their own directors, stakeholders and clients. This can save a lot of time, cost and disruption for both the auditing and audited parties – a benefit that contributes to the uptake of ISO27001-accredited certification.

However, claims of ISO27001 certification are often misinterpreted, or used as a guarantee where they should not be.

To gain certification, the organisation needs to comply with ISO27001, which means that it must have a scope defining the extent of its ISMS (or at least the extent of the ISMS that is certificated) and a statement of applicability (SoA) that defines

[12] To find out if an accredited certificate is the equivalent of those issued under the scheme described here, determine whether the accreditation body is a member of the International Accreditation Forum (www.iaf.nu)

what controls are applied across which aspects of the ISMS.

It is these two documents, together with the accredited certificate, that provide evidence of the level of assurance the organisation's ISMS provides regarding its information security practices.

ISO27001 is not a product certification scheme, and to rely on it as such is nonsensical. Certification to ISO27001 provides a service assurance.

Other audit applications

The provision of a specification for ISMSs lends itself to supplier or second-party audits. This means that buyers can rely on the standard to provide a recognised and widely available framework against which to conduct supplier audits in order to assure themselves of the level of security their suppliers are affording information that is provided as a result of the contract between the two organisations.

Second-party audits can be used by both the auditing and audited parties along similar lines as first-party (see Internal audits in *Chapter 3*) and third-party (see Certification audits in this chapter) audits, benefiting both organisations and driving continuous improvement through the supply chain.

CHAPTER 7: SIGNPOSTING

For access to a comprehensive set of all things relating to information security, and an impressive set of links to other sites, see

www.itgovernance.co.uk.

For general advice that is as applicable to the home as the office take a look at

www.getsafeonline.org.

Terms

Definitions that have been taken from ISO/IEC 27002:2005 are identified thus: *

Definitions that have been taken from ISO/IEC 27001:2005 are identified thus: **

Additional definitions that have been taken from BS7799-3:2006 are identified thus: ***

Definitions that have been taken from ISO/IEC 20000-1:2005 are identified thus: ****

Accreditation: the procedure through which an authoritative body formally recognises a person's or organisation's competence to carry out specified tasks. Not to be confused with certification. Third-party certification (auditing) bodies become accredited and those they audit, subject to a successful outcome, become certificated.

Asset: anything that has value to the organisation.* Information assets are likely to be of the following types:

- Information: databases and data files, other files and copies of plans, system documentation, original user manuals, original training material, operational or other support procedures, continuity plans, other fall-back arrangements, archived information, financial and accounting information.
- Software: application software, operating and system software, development tools and utilities, e-learning assets, network tools and utilities.
- Physical assets: computer equipment (including workstations, notebooks, PDAs, monitors, modems, scanning machines, printers), communications equipment (routers, mobile phones, PABXs, fax machines, answering machines, voice conferencing units, etc.), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, lighting, other equipment.
- Services: 'groups of assets which act together to provide a particular function', such as computing and communications services and general utilities, e.g. heating, lighting, power, air-conditioning.

Availability: ensuring that authorised users have access to information and associated assets when required.**

Certification: the process through which a certification body confirms that a product, process or service conforms to a specific standard or specification. For example, an organisation becomes certificated to ISO27001:2005.

Certification body: *see* Third-Party certification body.

Compliance: a positive answer to the question 'Is what is taking place in line with the pre-specified requirements for what should take place?' Hence non-compliance and compliance monitoring. Compliance is often used in a legal context.

Conformance: fulfilment of a requirement. A positive answer to the question 'Is what is taking place in line with the pre-specified requirements for what should take place?' Hence non-conformance and conformance monitoring. Conformance is often used in a non-legal context.

Document control: a system whereby all documents within the system have a standard numbering system that identifies where they sit within that system, as well as a version number, an issue date and a document owner, so that the currency of the document is always clear. When a controlled document is amended, all copies of it should be simultaneously withdrawn and replaced by the new version.

Encryption: the conversion of plain text into code, using a mathematical algorithm, to prevent it being read by a third party.

Information security event: an identified occurrence in a system, service or network indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security-relevant.* (*See also* Information security incident).

Information security incident: an unwanted or unexpected single event or series of events that have a significant probability of compromising business operations and threatening information security.*

Information security management system (ISMS): that part of the overall management system, based on a business risk approach, that establishes, implements, operates, monitors, reviews, maintains and improves information security.**

Information security policy: the organisation's policy for securing its information assets.

ISMS: *see* Information security management system.

ISO: acronym, from the Greek *isos* ('equal to'), adopted by the International Organisation for Standardisation – the world's largest developer of standards. Its membership comprises the national-standards bodies of countries around the world.

ISO27002:2005: the international code of best practice for information security which underpins and provides guidance for the implementation of an ISMS, specifically the revised version issued in 2005. It includes individual information security controls, implementation guidance and other information relating to these.

IT governance: a framework for standards of leadership, organisational structure and business processes, and for compliance with these standards, which ensures that the organisation's IT supports and enables the achievement of its strategies and objectives.

Policy: overall intention and direction as formally expressed by management.*

Project governance: the framework and rules controlling how project decisions are made and project activity monitored.

Registrar: Americanism for certification body; *see* Certification body.

Risk: combination of the probability of an event and its consequence.*

Risk acceptance: decision to accept a risk.***

Risk analysis: systematic use of information to identify sources and to estimate risk.*

Risk appetite: an organisation's overall attitude to risk, the balance between risk and return, and the trade-off between security and flexibility, usually a strategic decision by the organisation's board.

Risk assessment: overall process of risk analysis and risk evaluation.*

Risk management: coordinated activities to direct and control an organisation with respect to risk (usually includes risk assessment, risk treatment, risk acceptance and risk communication).*

SoA: *see* Statement of Applicability.

Statement of Applicability (SoA): document describing the controls and control objectives that are relevant and applicable to the organisation's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.**

Third-party certification body: independent organisation with the necessary competence and

reliability to award certificates following verification of conformance. It is advisable to check the accreditation status of such bodies prior to appointing them.

Threat: a potential cause of an unwanted incident, which may result in harm to a system or organisation.*

UKAS: United Kingdom Accreditation Service – the sole national accreditation body recognised by the UK government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services. *www.ukas.com*.

Vulnerability: a weakness of an asset or group of assets that can be exploited by a threat.* There are regularly updated central stores of known vulnerabilities at Bugtraq (*www.securityfocus.com/archive/1*), CVE (Common Vulnerabilities and Exposures – *http://cve.mitre.org/*) and in the SANS top 20 (SANS (SysAdmin, Audit, Network, Security) Institute – *www.sans.org/top20/*).

ITG RESOURCES

IT Governance Ltd source, create and deliver products and services to meet the real-world, evolving IT governance needs of today's organisations, directors, managers and practitioners. The ITG website (*www.itgovernance.co.uk*) is the international one-stop-shop for corporate and IT governance information, advice, guidance, books, tools, training and consultancy.

Copies of all the standards described in this pocket guide can and should be purchased from *www.itgovernance.co.uk/standards.aspx*.

www.27001.com is the IT Governance Ltd website that deals specifically with information security issues and these information security standards. While it has a specific US orientation, it supports ISO27001 activity around the world. It also has a links page that lists accredited certification bodies and international ISMS user groups.

Pocket Guides

For full details of the entire range of Pocket Guides, simply follow the links at *www.itgovernance.co.uk/publishing.aspx*.

Toolkits

ITG's unique range of toolkits includes the ISO27001 ISMS Toolkit, which contains all the tools and guidance that you will need in order to develop and implement an appropriate ISO27001 ISMS for your organisation. Full details and a free trial can be found at *http://www.27001.com/ISMSFreeDemo.aspx*.

For a free paper on how to implement ISO27001 in your organisation, there is a free download available on the home page of *www.27001.com*.

Best Practice Reports

ITG's new range of Best Practice Reports is now at *www.itgovernance.co.uk/best-practice-reports.aspx*. These offer you essential, pertinent, expertly researched information on an increasing number of key issues.

Training and Consultancy

IT Governance also offers training and consultancy services across the entire spectrum of disciplines in the information governance arena. Details of training courses can be accessed at *www.itgovernance.co.uk/training.aspx* and descriptions of our consultancy services can be found at *http://www.itgovernance.co.uk/consulting.aspx*.

Why not contact us to see how we could help you and your organisation?

Newsletter

IT governance is one of the hottest topics in business today, not least because it is also the fastest moving, so what better way to keep up than by subscribing to ITG's free monthly newsletter *Sentinel*? It provides monthly updates and resources across the whole spectrum of IT governance subject matter, including risk management, information security, ITIL and IT service management, project governance, compliance and so much more. Subscribe for your free copy at: *www.itgovernance.co.uk/newsletter.aspx*.