COMP61421 *Notes for days 1 and 2, and coursework I*

Cyber Security: *From Risk to Treatment*

Dear Student of Information and Cyber Security,

You will already be muttering that this module is about *cyber* not *information* security so why is he calling me a student of something else? I am not. The secret of all this is to remember what problems are, might be, have been, and how to deal with them. With the right attitude, the rest will follow.

So…when you panic over the republication of our guiding beacon BS ISO/IEC 27001 in its 2013 revision, when you wonder what IASME is, and you regret your decision to click on the print button for NIST SP 800-50…don't panic (Adams, 1978)!

The Standards Coordination Group of the Trusted Software Initiative[1] recognized that 'cyber security' is without a generally accepted definition; different standards makers use different definitions. It is our observation that cyber and information security are two different things. And this is why it is perhaps not surprising that those who appreciate the history (Williams, 2013) are unhappy with the term 'cyber' being appended to all things touching on information technology in general and the Internet in particular. Production lines, SCADA[2] operation, medical records, credit card numbers, credentials, military equipment and such, need to be protected[3]. Where we are interested in the behaviour of the system - and the necessary monitoring and protective or corrective feedback - then it is cyber and it is permissible to borrow the term (from Weiner, 1948). So when the SCADA engineers talk about cyber security, they really mean it[4].

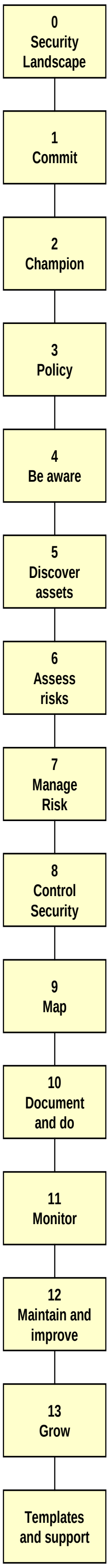
For the purposes of this module, we will use computer and network security, information security, information assurance, and cyber security with reckless interchangeability. We shall temper this unscientific behaviour by awarding them all a common definition:

…the assurance of confidentiality, integrity, and availability
of information stored and processed
on electronic devices which may be interconnected…

Things change. Stuff happens. You are an MSc student. Synthesising the *now* from the *was* and the *will be* is your bread and butter…or mother hood and apple pie if you prefer. (I prefer apple crumble and that has nothing to do with the almost universal symbolism of the fruit.)

This book…all the slides in the lecturers…and my words are for guidance only. It's your decisions as you go out from here to direct a team, code an application, or engineer a system, that matters. Can-do attitudes this way please.

Dr Daniel G. Dresner
University of Manchester
Autumn 2016



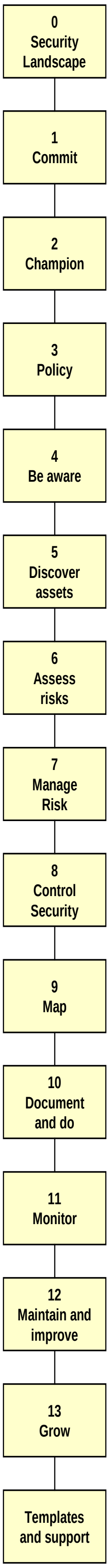
[1] http://www.uk-tsi.org.uk/

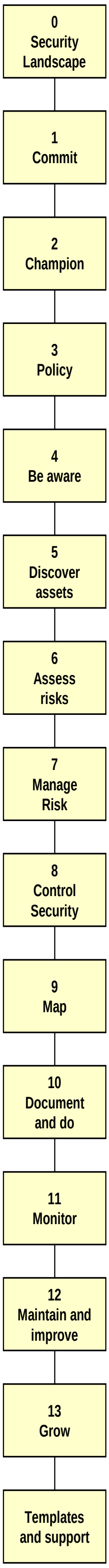
[2] Supervisory Control And Data Acquisition [systems]

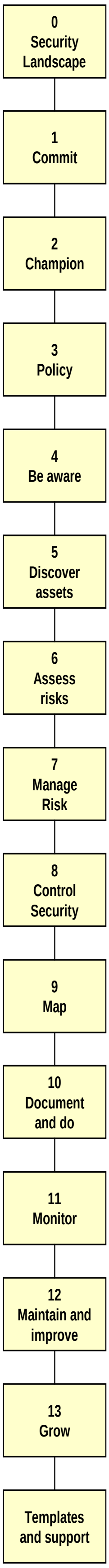
[3] That is, in a state of information security.

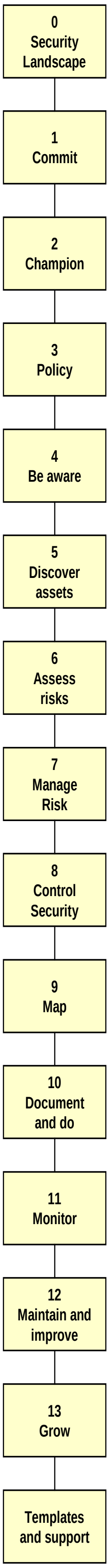
[4] Essential reading! *The three laws of cyber and information security* http://www.softbox.co.uk/pub/threelawsofcybersecurity_dgd13a_nj10.pdf

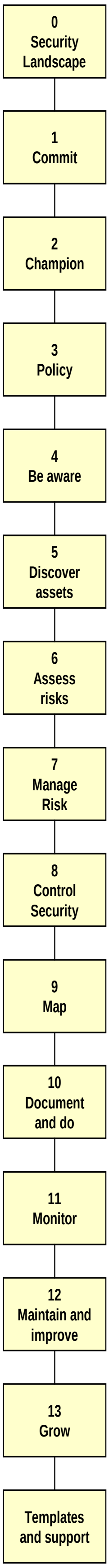
Contents


0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support


0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support


0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support


0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support


0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

List of Figures

List of Tables

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

1. Introduction: information and cyber security risk

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Information is the lifeblood of all businesses. And just because we may have got away without identity theft or our PCs being used to cache pornography, we should also heed the warnings of what can be done with the information we treasure and the resources we invest in. Information, ranging from details about clients to confidential intellectual property, from budget projections to employees bank account numbers, suffuses all parts of any organisation, regardless of size, sector, or purpose. There are risks to our business information that must be mitigated or reduced to acceptable levels.

Just like any other asset, information must be protected. It may be stolen or sabotaged. It may be unavailable at the very time it is needed. Furthermore, we have legal obligations to provide adequate protection to some types of information. If this is not enough, if others use our resources for their misdemeanours, we may be liable if we did not try to at least pre-empt their actions.

Failure to protect information from loss and the cause of loss, will inevitably lead to erosion of the trust that an organisation has built up with its customers and trading partners. Some failures – particularly those with a high media interest, such as hacking or money laundering – can equally result in public relations disaster.

As systems grow in complexity, deperimeterisation becomes ever more prevalent with cloud and grid services consumed by tablets and mobile telephone, we can no longer rely on setting up the controls architecture for one monolithic organisation. Organisations are part of supply chains that use applications and data drawn from and store in applications and data clouds. Information needs protecting as it passes through static and mobile storage and processing devices, the Internet, operating systems and application software. Controls need to be selected judiciously to contain the risks to this information within a changing envelope of acceptable risk.

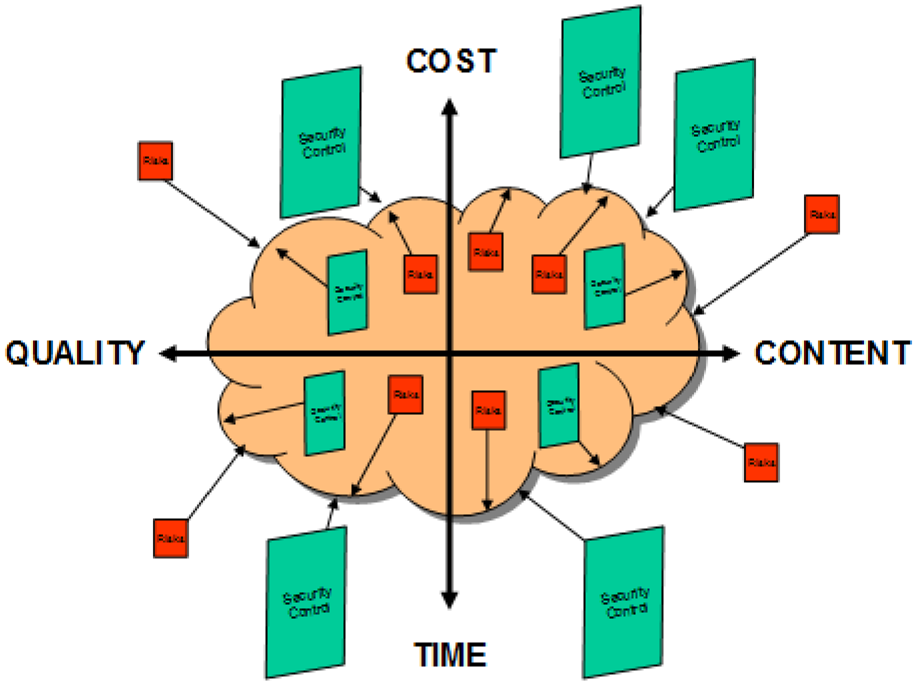


Figure 1: Shaping the envelope of acceptable risk

For any organisation to function reliably, therefore, its information must be protected from risks in three key areas:

- **Confidentiality** – Some information is suitable for dissemination to the public or to clients; other information may be highly confidential to a few individuals within an organisation. It is necessary to devise a system for setting a level of confidentiality on all information, labelling it in a consistent and visible manner, and ensuring that those without the appropriate level of privilege cannot access the information.

- **Availability** – The most frustrating words for any customer of any organisation are, "I'm sorry, but the system is down right now". Information owners are expected to put measures in place to ensure that their information will be available as staff and customers expect it to be.
- **Integrity** – Staff, clients, citizens and other stakeholders must be able to trust the information that they are basing their decisions on to be accurate, complete and up-to-date.

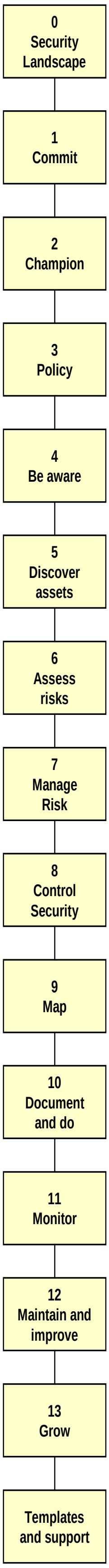
By paying strict attention to the tools that make security meaningful:

- **Authentication** – Being assured of the identity of those with whom you're dealing is more difficult, the less direct contact your senses have with them. There are too many criminals who take advantage of this. Identity management has never been more important.
- **Authorisation** – Knowing identity is the beginning of security. Knowing what that identity is allowed to have access to is the next phase. A basic tenant of security management is to keep authentication and authorisation separate.
- **Non-repudiation** – So you know who it is and what they may have access to but do you know where they've been and what they've done whilst there? Evidence for some basic forensics may be needed in what may start as the most innocuous of situations but change irrevocably in a case of misuse.
- **Trust** – Different sizes of organisation will feel that different approaches to trust are appropriate. As one colleague has bluntly described it: 'trust is not a control'. Trust is where you decide to accept risk.
- **Confidence** – With risks assessed, controls accepted and trust instilled, the stakeholders will have the confidence they need to use the information systems at hand, until incidents suggest that they may be unwise to do so. Losing confidence means not being ready for those incidents and facing costly reappraisal of risks to regain trust (sometimes irrevocably lost) and try to rebuild confidence.

This is made no simpler by the realisation of many that information has a lifecycle and its audience will vary from the time a concept is developed in secret through to its internal distribution, its release into the public domain, and the possible need to revoke or replace it. There's a balance to be drawn and risks to be assessed. The oft attributed quote eloquently describes the flow of information, 'a lie can get halfway around the world whilst the truth is still putting its boots on'.

The purpose of the International Information Security standard, ISO/IEC 27001[5], is to set out a framework of controls that an organisation can use manage risk with an information security management system (ISMS). The complementary family of standards developing around it provide a systematic approach to the creation and maintenance of the key documents, processes, checks and balances and training materials needed for the effective management of information security.

ISO/IEC 27001 is a scalable standard. The challenge faced by its creators was to devise something that would be equally suitable for a micro business and a 40,000 person multinational corporation. Hence, rather than provide a model ISMS, it specifies the method by which each organisation can develop their own. This extra layer of abstraction makes the standard almost universal.



[5] The numbering of standards is not a dark art. However, we need a protective charm to prevent us being distracted from the objective of information security by the original BS 7799 (a British Standard) being split into different parts, one of which became ISO/IEC 17799, each of which will become known by its place in the ISO/IEC 27000 series. Our convention will be to refer to ISO/IEC 27001 throughout this guide when we talk about processes and ISO/IEC 17799 when we talk about putting security controls in place. This is not a bad convention because the contents of ISO/IEC 27001 straddle all of the other standards in the field of information security (at least implicitly) and guide you in the customisation of the controls (ISO/IEC 27002) for your circumstances. Stay calm: ISO/IEC 17799 became ISO 27002, it's only a number!

This Best Practice Guide addresses the stages that an organisation must go through when developing their own ISMS or assuring the future of any effective ISMS that they already have in place. It examines the various processes, and their business implications – for example, the likely cost, timescales, and political impact. It recommends the deliverables that will have the greatest value. Finally, it discusses the options for keeping the ISMS current, to prevent the whole process having to be repeated, from scratch, a few years down the line.

Note: This best practice guide is all about implementing the most appropriate standards. We focus on the developing ISO/IEC 27000 series of standards and refer to some other helpful guidance along the way. However, the guide does not repeat all the lessons therein. There is no substitute for reading the standard in its original form, and since the 2005 version was created with readability and understandability in mind, there are no excuses either. However, to retain a degree of verisimilitude with the sources for our guidance, we make copious reference to the baseline documentation.

1.1. What is Information?

What is information? In the simplest terms, it is organised data – collected, processed, and stored so that it can be retrieved in order to help in the making of a decision. This definition applies, whether the information is aimed at management (‘How many new staff must I employ?’), staff (‘Am I allowed to give a discount on this product?’) or customers (‘Should I buy this laptop, or that one?’).

Information exists in many formats. It is written or printed on paper; it is stored on hard discs, floppy discs, CD-ROMs, and USB drives; it is held in peoples’ brains. It is ubiquitous, and most organisations nowadays spend a vast amount of their employees’ time handling information, processing, changing and passing it on.

Information may be the variable that causes change or regulation to occur in a process which may itself be driven by information technology. Monitoring the effect that this has may give rise to changing information that in turn affects the process. This is feedback and we must take an interest in the effect on the cybernetics that tampering with the information can effect. This is the realm of cyber security.

The ease with which information can be shared has changed the economy completely in a fairly short time. It has created new opportunities, new marketplaces, and new ways of doing business. It has increased cash flow, and it has increased quality. But it has also created an evolving range of threats to the businesses that rely on it.

The existence of these evolving threats means that protecting information is no longer a matter simply of common sense, and it is no longer something that can be done reactively in response to a perceived threat. It is essential that a structured framework of controls and guards be put in place. It is this Information Security Management System (ISMS) that ISO/IEC 27001 seeks to standardise.

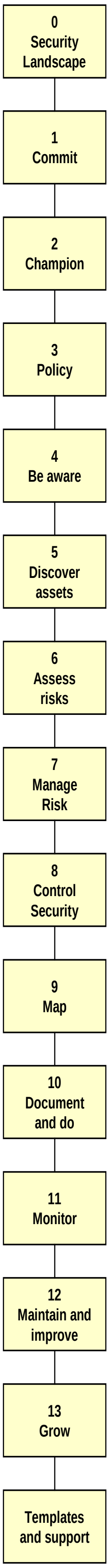
1.2. What is Information Security?

According to ISO/IEC 27002:2005, information security is the preservation of confidentiality (ensuring that the information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required) of information. It goes on to add that other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

This is an overarching definition. Nevertheless, it encompasses an enormous variety of threats – from hackers to power-cuts; from disgruntled employees to inadequately-trained programmers.

1.3. Risks faced in IS/IT

In 2005, The National Computing Centre researched the top ten IS/IT risks in information as part of a wider project looking at standards and risk inspired by the need of the financial sector to comply with



the second Basel Accord of the Bank of International Settlements. The catalogue of risks that was drawn up is an adaptable set of classifications rather than headline grabbing cries of woe over (for example) wireless connections and instant messaging. At the very heart of this research is the derivation of more evidence for the usefulness of ISO/IEC 27001 and other management standards.

Rank	**Risk**	**Details**
1	Unacceptable use by or through staff, contractors, partners, and former employees.	This category of risk has similar properties to the category of holes punched through established defences. It refers to the deliberate or accidental misuse of appropriately granted privileges with both innocent and malicious intent by those with permission to be where they are.
2	Complacency, lack of awareness or understanding of risks, or accepting too much risk.	Unless the chance of a risk can be reduced to zero – at which point it may be argued that it is no longer a risk – there must be some level of acceptance. This may be a deliberate act or through ignorance.
3	Breaches in established defences, poor/changes to configuration without risk analysis.	Simple onion-skin models[6] for access to information systems become less effective with the autonomy given to legitimate users. People, other systems, or software applications that are allowed permission into the defined periphery and may allow inappropriate traffic through that cannot easily be differentiated from legitimate activity[7].
4	Systems lifecycle management, poor requirements definition. Poor system design and inadequate testing.	In 1988, research[8] commissioned by the UK Department of Trade and Industry estimated the annual loss to the UK economy resulting from defects in domestically produced software sold on the open market to be £600 million. A complementary report[9] indicated that quality risks in software development could be mitigated by implementing ISO 9000 (which was BS 5750 at the time and is now ISO 9001) for Quality Systems and being independently certificated for it. The information technology certification scheme designed to encourage this peaked at a little over 1700 certifications and had dropped to less than 1300 by 2005[10].
5	Inadequate resilience, poor business continuity management.	Business continuity plans should not be expected to pre-empt every eventuality[11] (or emergent risk) but rather provide a framework of mitigating action based on the probability (risk) of incidents from a risk assessment or treatment plans.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[6] Ian F. Alexander, *A Taxonomy of Stakeholders: Human Roles in System Development*, 2005

[7] The National Computing Centre, *Guideline 289: Protect and Survive - Defending against application hacking*, 2004

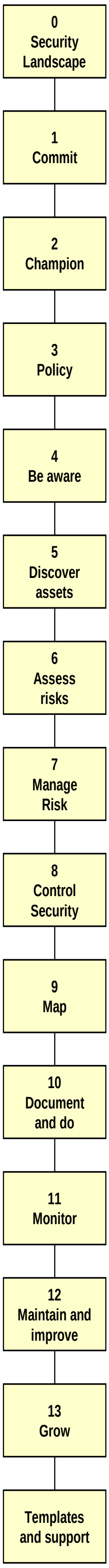
[8] Price Waterhouse, *Software Quality Standards: the Costs and Benefits*, 1988

[9] Logica, *Quality Management Standards for Software*, 1987

[10] www.tickit.org

[11] Armstrong, J., Rhys-Jones; M., Dresner, D., *Managing Risk: Technology and Communications*, Lexis Nexis, 2004

Rank	Risk	Details
6	Sabotage of data or systems, malicious software.	There are several variations on the theme of malicious code. Worms permeate computer systems, changing code and erasing files. They are difficult to trace and stop. Macro viruses hide within applications files such as spreadsheets or word processor documents, and their damage can extend well beyond the application. Trojan Horses, like their legendary namesake, hold hidden problems within an otherwise innocent looking file. They breakdown defences to enable unauthorised access to the network.
	Governance weaknesses, lack of legal and regulatory compliance.	The spectacular collapse of major organisations through fraudulent financial reporting has prompted attention to the internal controls that manage operational risk[12] so the implied requirements of good governance are now a statute in the US[13] and benchmarks for corporate regulation in the UK[14]. Banking has also introduced its own risk management framework[15].
7	Unauthorised access, fraud, identity theft.	The value of information assets may be measured in several different ways varying from the focused total cost of ownership of hardware and software[16] to including the calculation of the value of intangible assets such as intellectual property[17]. This may be extended to very personal losses through the targeted theft of very specific items of identification that allow inappropriate access to bank accounts.
8	Lack of professional, affordable IS/IT risk mitigation specialists to advise on and implement risk reduction plans.	The step by step advice in this best practice guide is firmly in line with the idea of where you lack the time or expertise in your own organisation to solve a problem, you need someone to call. Hereon in, we've referred to this person as the security expert. For many this will be a consultant and knowledge is a commodity. Security experts have invested in their knowledge and will want to reap the rewards. The problem being is that many organisations cannot budget for a fair price, especially when it may be difficult to quantify the return on investment to the board.



[12] Armstrong, J., Rhys-Jones; M., Dresner, D., *Managing Risk: Technology and Communications*, Lexis Nexis, 2004

[13] Public Company Accounting Reform and Investor Protector Act of 2002 (commonly referred to as Sarbanes-Oxley). Section 404 requires board level certification of an organisation's financial activity and the effectiveness and status of the organisations internal controls.

[14] Sir Adrian Cadbury's 'The Financial Aspects of Corporate Governance', 'Internal Control: Guidance for Directors on the Combined Code' popularly known as the 'Turnbull Report' and the Higgs Report which reviewed the roles and effectiveness of non-executive directors.

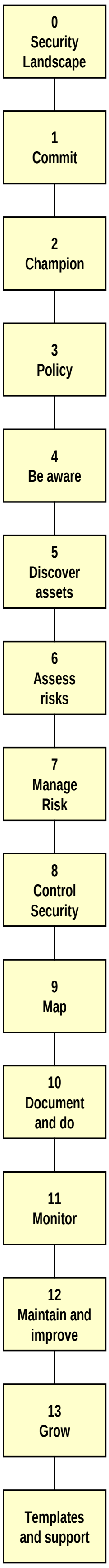
[15] The second Basel Accord of the Bank of International Settlements (Basel II)

[16] Gartner Group, 1987

[17] Thomas A. Stewart, *Intellectual Capital: The new wealth of organizations*, Nicholas Brealey 1997

Rank	Risk	Details
9	Loss of key resource - staff/supplier relationships.	There was once a time when organisations would pose questions of what they might do if certain ‘key’ staff – and here we are talking about the overstretched IT manager, or support staff, not one of those smaller stones at the top of pyramid – got knocked down by a bus or win the lottery and disappear off into the proverbial sunset. Whatever the urban legend, few jobs involved in maintaining the integrity and availability of information can be done by numbers; it’s a combination of skills, competency, and well documented processes. Documentation is only a component; when service level agreements are waved in anger, their contribution to the goals of the organisation falls exponentially. It has been observed that organisations work more on the management and development of relationships rather than the achievement of absolute goals. The objectives are achieved by the realisation of these relationships. The risk is therefore when these relationships teeter.

Table 1: The results of the NCC survey into the top risks in IS/IT



1.4. What are all these numbers?

1.4.1. History

Information security used to be simple and straightforward. All that was required was a good sturdy filing cabinet and a burglar alarm. The only way to illicitly acquire a business’s intellectual property was to break into their offices and make off with floppy discs or PCs. People were aware of hackers, dimly, as individuals likely to read the Duke of Edinburgh’s e-mail on Prestel, or maybe start world war three during a slow afternoon.

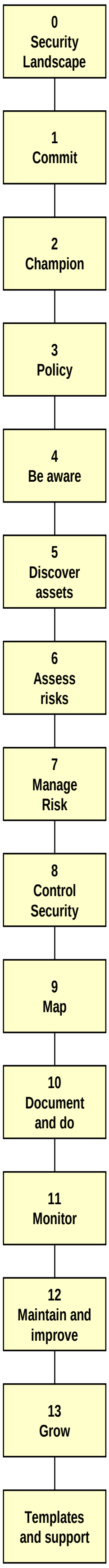
And then, in the early 1990s, everything changed. Some pioneering companies started offering access to the Internet to the general public and suddenly it was open season on networks that had previously been largely safe and trusted.

The UK Department of Trade and Industry (DTI) began a campaign to raise awareness of the importance of information security in this new environment. The National Computing Centre (NCC) performed a survey in 1994, and the results were stark: information was under threat like never before, and the threat was – to a large extent – not being adequately managed (or in some cases, not being managed at all).

The DTI responded by publishing a code of practice, which was swiftly worked into a formal British Standard for Information Security Management (BS 7799), which saw the light of day in 1995. BS 7799 was issued in two parts. Part 1 was the code of practice itself: the baseline of best practice and set out what needs to be controlled to manage information security. Part 2 was a specification for information security management systems, and dealt with the practicalities of applying the best practice documented in part 1.

The first release of the British Standard was criticised as being overly simplistic. In 1999 the document was comprehensively revised, and the new release of the Standard was considered extremely comprehensive and well thought out. In recognition of this it was adopted, virtually unchanged, by other standards bodies around the world, for example Standards Australia and

Standards New Zealand. Critically, for widespread acceptance, the International Standards Organisation (ISO) also took part 1 (that's the catalogue of controls) on board and released it – with a few revisions – as ISO/IEC 27002 in 2002. It's the 2005 version of this that has inspired this guide (but note that it's not the latest version). Together with ISO/IEC 27001 – the development of BS 7799 Part 2 (that's the part against which an organisation can be audited and certificated for compliance) - ISO/IEC 27002 is becoming a component of an multi-part, highly practical and usable set of standards for the aspiring and succeeding information economies.



1.5. What is ISO/IEC 27002[18] for?

ISO/IEC 27002 has often been rejected by those with polarised views of how information security ought to be handled. Its commitments scare those who think the standard aims for too much security. Open it and have a look; there are 135 security measures in there. For the small business that sees risk in terms of pleasing a key customer or satisfying the bank that cash flow is under control, the risks of information security are likely to be classed as those one could get away without doing anything about. There is often too much of the wood of potential distractions to see the trees of assurance.

On the other side of that same coin, there are the organisations who know that their industrial process or chemical recipe is just so vital that it cannot be left to a standard that has not been created especially for them. They think it's not secure enough.

And we can sympathise with these worries. Standards have received a bad press over the years as critics are quick to point the finger of blame rather than grasp the laurel wreath to crown the victors of implementation. But both the advocates of 'too much' or 'too little' are failing to see that they are actually promoting the ethos of ISO/IEC 27001/27002. The standard is scalable. It is risk-based. We all face different risks. ISO/IEC 27002 helps us to reduce them to an acceptable level in whatever we do. One 'caveat': look at the risk ranked as second in the table above.

The potential audience for ISO/IEC 27002 is extraordinarily broad; this is deliberate. It was not developed with any particular scale or sector of organisation as an intended target. This is something of an achievement in itself – how much commonality, after all, can there be between the information security management requirements of a three-person small business selling toys and a defence contractor with 40,000 employees?

The answer, once again, lies in the fact that ISO/IEC 27001 and ISO/IEC 27002 do not prescribe a one-size-fits-all information security management system. They are a **standard framework** for the creation of an information security management system.

The finished product – the ISMS itself – will naturally exist on a number of different scales – perhaps manifesting only a few dozen pages in three or four documents for the smaller end of the range, right up to a sophisticated intranet in the largest of businesses. The process, by which appropriate documentary tools are created, however, is remarkably similar, and it is this process that these best practice guidelines relate.

The core strength of ISO/IEC 27002, which will be discussed further, lies in the compliance process which involves choosing which sections of the standard – or strictly speaking, code of practice - apply to the particular organisation in which the ISMS is implemented (using the risk assessment process of ISO/IEC 27001). Most organisations will not need to use every control in the standard. The vast majority of organisations will be able to perform a risk analysis pretty quickly using no more tools than plain common sense. Some organisations will doubtless need to plan for the many eventualities – think about the Civil Contingencies Act (CCA) - but the rest will be able to skip unrequired sections (documenting the decision to do so) and move on to the next without in any way compromising their compliance – or chances of certification – to the standard. Get over the scale of the standard; do not let

[18] Remember, don't worry about whether you call it ISO/IEC 17799, BS 7799 Part 1, or ISO 27002. It's the contents that are important. What is important is to keep up to date with developments and ensure you are referring to the latest version. Refer to the standards catalogue on www.bsi-global.com.

it be intimidating; there are very few situations in which an organisation may legitimately decide that it is ‘not for them’. It breaks bigger obligations such as CCA, or Sarbanes Oxley compliance, into manageable chunks.

1.5.1. Benefits of application

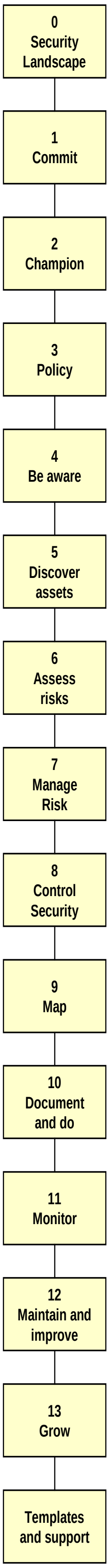
Physical security is a relatively simple matter, because it is founded in the physical world – a place that everyone can relate to. The measures needed to protect physical assets, therefore, are easy to suggest, because it is equally easy to understand the threats. Everyone locks and unlocks doors many times a day, so such precautions as sturdy locks, burglar alarms, and strong cabinets are seen as little more than common sense.

The same cannot be said about information security. People unfamiliar with the architecture, design and maintenance of information systems will not be able to define the threats and vulnerabilities that they face in any more than the haziest terms. This is a serious problem to any organisation, because this applies – all too often – to those tasked with making critical and strategic decisions: top management and shareholders, for example.

This suggests a need for all organisations to put a formal framework in place for managing their information systems, because ad hoc management, clearly, will be patchy, unreliable, and subject to the impact of poor decision making. This much has been understood for many years. ISO/IEC 27001 and ISO/IEC 27002 simply provide the extra benefit of a specification – devised and reviewed by the industry’s experts – for such a framework. The adoption of this framework makes a clear statement – that the organisation understands the need to protect its information assets, and that such protection will be implemented to an internationally recognised standard. With a standard ISMS in place, the uncertainty can recede; replaced by an independent model for information security in which managers, shareholders, staff and clients can all have confidence. And this international status is encouraging as it is often hard to justify prevention because you will not be able to show the after effects which prove your case. The famous ‘Millennium Bug’ is a case in point. The International efforts put in were successful in mitigating the potential disaster. Now – like the fate of the Pied Piper – the fashion is to think that there was no disaster. We don’t stop inoculation programmes because no one is becoming ill. That is until, like small pox, the problem is eradicated. The computer virus is still going strong and has become a euphemism for all sorts of computer ‘malware’.

It is important to manage expectations, of course. Nothing can ever be totally secure. Even the most solidly constructed firewall can be circumvented if the value of the information on the other side merits such effort. We have seen above that the complexity of information systems may be the weakness and malicious activity may be channelled through an established defence like a firewall posing as part of a legitimate application. Furthermore, security is always a compromise between the safety of the information and the needs of the business. However, as long as the controls in the ISMS are applied properly, fully, and consistently, the risk to the protected information will be vastly reduced. Compliance to ISO/IEC 27001 doesn’t guarantee the safety of information, but it does show that best practice has been followed.

Once you have implemented a compliant ISMS, it should be desirable to take the next logical step – to apply for certification. It encourages fresh thinking and steers you away from the risk (sic!) of complacency. Certification opens up a potential range of other benefits. It used to be the case, for example, that each organisation was master of their own information security. In the knowledge economy of B2B e-commerce trading and extranets, the weakest point in any network of networks may actually be in a supply chain partner’s system. It is necessary to grant these partners a certain degree of access to information, but it is also necessary to trust them not to expose said information through their own oversights. More and more businesses now are requiring that such e-commerce partners demonstrate compliance with ISO/IEC 27001 before such trusted connections are established. Customers, too, will show increased confidence to do business with an organisation displaying the coveted badge of ISO/IEC 27001 certification. Survey after survey shows that fear of fraud is still a major factor in discouraging electronic transactions, and certification to a known standard is an



excellent way to build integrity and trust between a supplier and its clients. Furthermore, insurance against loss or damage to information, and the potential liability that is associated with it, is increasingly common in business now, and it is likely that the premiums involved will be much lower if an organisation's ISMS is accredited. It may become a pre-requisite for some forms of insurance.

1.5.2. Quantifying the benefits

Information security is a good example of what workplace psychologist Frederick Herzberg called a 'hygiene factor'.

Originally this term was used for motivational theory, to describe the factors that do not have tangible benefits when present, but lead to dissatisfaction when omitted. The example he used, from which the concept gets its name, was washrooms. If the washrooms in a business are filthy, with cold water, and old, damp towels then the negative impact is obvious. If the same facilities are overhauled and made acceptably clean, and acceptably well maintained then the negative impact is removed, but no positive impact can be observed. If the facilities are then improved further – gold plated taps, for example, and valets to distribute luxurious thick towels – still no positive impact will be observed.

Information security is similar. If it is neglected then the list of possible negative outcomes is vast – in fact, the business could be destroyed outright. If it is properly implemented then the best possible outcome is that no incidents occur. It does not matter whether the bare minimum has been implemented, or if the ISMS is all-encompassing, finely detailed, and regularly reviewed. The best possible result is still that no incidents occur. Of course, the same applies to physical security.

This lack of opportunity to meaningfully quantify the benefits of a well-designed ISMS is another reason for adopting the explicit experiences embodied in ISO/IEC 27001 and ISO/IEC 27002. Such a move goes a long way to alleviate anxiety that the only reason for a lack of incidents so far has been more due to luck than to a totally comprehensive approach to protection.

1.5.3. ISO/IEC 27002:2005 – section by section

In this part of the guide we look at the contents of the standard catalogue of controls, but only briefly. There is no substitute for working from the source. We also keep one eye on the previous issue of ISO/IEC 17799 (BS 7799 Part 1 - see the table below) to give an anchor point for those who have worked with the standard for years. It may also be of interest to the newly initiated as it shows how a standard develops with time.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Main contents of ISO/IEC 27002:2013[19]	Main contents of ISO/IEC 27002:2005	Main contents of ISO/IEC 17799:2000
	Risk Assessment and Treatment	
Information security policies	Security Policy	Security Policy
Organisation of information security	Organising Information Security	Security Organisation
Human resource security		
Asset management	Asset Management	Asset Classification and Control
Access control		
Cryptography		
	Human Resources Security	Personnel Security
Physical and Environmental Security	Physical and Environmental Security	Physical and Environmental Security
Operations security		
Communications security	Communications and Operations Management	Computer and Operations Management
System acquisition, development and maintenance		
Supplier relationships		
	Access Control	System Access Control
	Information Systems Acquisition, Development and Maintenance	System Development and Maintenance
Information Security Incident Management	Information Security Incident Management	
Information security aspects of business continuity management	Business Continuity Management	Business Continuity Planning
Compliance	Compliance	Compliance

Table 2: A comparison of the 2013, 2000, and 2005 editions of ISO/IEC 27002 (17799)

The sections of controls set out in ISO/IEC 27002 do not deal with completely isolated requirements; there are a number of common themes that emerge as they are examined. Of these themes, the one that is stressed most frequently is the requirement to plan ahead for security issues.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[19] BS ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

1.5.3.1. Structure of the ISO/IEC 27002 standard

The International Standards Organisation really does have a ‘standard for standards’ so if you’ve looked at other standards you will be at home with this one. Where this standard – and indeed others – have learnt from the unfortunate reputation of their predecessors is in the inclusion of explanatory material to introduce readers – or rather standards implementers – to the background of the demand that the standard goes on to make for compliance.

So, in the opening of the standard you will find consideration of the following questions and activities:

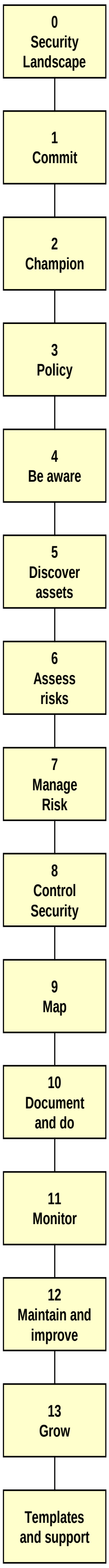
- What is information security?
- Why information security is needed
- How to establish security requirements
- Assessing security risks
- Selecting controls
- Information security starting point
- Critical success factors
- Developing your own guidelines

Then after looking at the scope of the standard and making the use of terms and definitions clear, the standard goes on to cover . . .

1.5.3.2. Risk assessment and treatment

If there is one part of the standard that you could read and throw away the rest it is this section. The late Douglas Adams once surmised that because of the gravitational interaction of all matter you could extrapolate the entire structure of the universe from a small piece of fairy cake. In the same way, you should – **if you are honest enough to yourself and your stakeholders** – be able to extrapolate all the security measures you will ever need by considering what the risks you face are and then decide what to do about them; that is, how to treat them so that you can reduce them to an acceptable level. This is why managing risk is the first key section of the standard and why a whole part of the developing suite of information assurance standards is being developed to help you with risk management techniques.

Although most definitions of risk tend to be most concerned with harm, loss, or danger[20], the risk management process is increasingly recognised as being concerned with both the positive as well as the negative aspects of uncertainties.[21] [22] [23] Similarly, if risk is viewed in terms of its outcomes, for example, losses and gains[24], definitions do little to separate hazards[25] or the causes of risks, from the actual ‘loss/gain’ risks themselves. The concept of risk as an ‘undesirable outcome’[26] can be a useful focus. A review of risk registers (which are discussed later) supports the assertion that there is usually poor differentiation between risk (as the outcome – the loss) and the cause(s) of the risk. Risk may be



[20] Houghton Miflin American Heritage Dictionary

[21] PD ISO/IEC Guide 73, Risk Management –Vocabulary – Guidelines for use in standards, British Standards Institution, 2002

[22] Department for Environment, Food and Rural Affairs, DEFRAS(2002)

[23] ALARM – the forum for risk management in the public sector, *A key to success - a guide to understanding and managing risk*, February 2001

[24] Ibid.

[25] Hazard is an event or situation which can cause harm (including ill health and injury; damage to property, plant, products or the environment; production or financial losses, increased liabilities, etc.). ALARM – the forum for risk management in the public sector, *A key to success - a guide to understanding and managing risk,* February 2001

[26] Swann, *The Economics of Standardization*, 2000

defined as a catch-all term pertaining to possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility[27].

Risk management is associated with good governance across corporate governance in all disciplines[28]. The idea of risk appears to have been coined first by 16th and 17th Century Western explorers. The word 'risk' seems to have come into English through Spanish or Portuguese, where it was used to refer to sailing into uncharted waters. It had an orientation to space, eventually being transferred to time, as used in banking and investment - to mean calculation of the probable consequences of investment decisions before referring to a wide range of other situations of uncertainty. There is no risk where an outcome is 100% certain.[29]

The Basel Committee for Banking Supervision (the self-regulating body for banking[30]) defines operational risk as:

> 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events'[31]

This definition is adopted widely in banking[32]. The challenge is how to model external events on processes, people and systems with a view to controlling the processes, people and systems and avoid undesirable outcomes and achieve positive results. Without effective and repeatable risk identification methods, truly effective risk management is impossible[33]. From which follows the need for a course of action to deal with the identified risks, or have them accepted by the respective, authoritative, stakeholders.

Other definitions model generic risk as a combination of consequence or impact and likelihood or probability.[34] [35] [36] [37] [38] [39] See this as being bounded by the project[40] envelope of cost, schedule, quality, or technical constraints[41] or applied directly to the security risks associated with information systems[42].

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[27] Jyrki Kontio, *The Riskit Method for Software Risk Management, version 1.00*, University of Maryland, 1998
[28] PD 6668 *Managing Risk for Corporate Governance*, British Standards Institution, 2001
[29] Professor Anthony Giddens, Reith Lectures, 1999
http://news.bbc.co.uk/hi/english/static/events/reith_99/week2/week2.htm
[30] The Basel Committee was established at the end of 1974 comprising of members from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States. Countries are represented by their central bank and also by the authority with formal responsibility for the prudential supervision of banking business where this is not the central bank.
The Committee formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements - statutory or otherwise - which are best suited to their own national systems. (www.bis.org)
[31] Harris, Rick, *Emerging Practices in Operational Risk Management*, Federal Reserve Bank of Chicago, 2002
[32] The Federal Reserve Bank of San Franscisco Economic Letter, Number 2002-02, January 25, 2002
[33] Marvin J. Carr, Suresh L. Konda, et al., *Taxonomy-Based Risk Identification*, Software Engineering Institute, June 2003
[34] PD ISO/IEC Guide 73, *Risk Management –Vocabulary – Guidelines for use in standards*, British Standards Institution, 2002
[35] Defense Contract Management Command, PROCAS; Online Information Center Summary Document, November 1999
[36] Financial Services Authority, *The firm risk assessment framework*, February 2003
[37] Australian Agency for International Development, *AusGUIDElines, 5. Managing risk*, The Australian Government's Overseas Aid Program, 2000
[38] IEEE Std 16085 (Previously IEEE Std. 1540-2001)- *IEEE Standard for Software Life Cycle Processes - Risk Management*, 2003
[39] PD 6668 *Managing Risk for Corporate Governance*, British Standards Institution, 2001
[40] BS IEC 62198 *Project risk management - Application guidelines*, British Standards Institution, 2001
[41] US Office of the Under Secretary of Defense (Acquisition, Technology and Logistics) / Defense Systems, 2004
[42] European Network and Information Security Agency, ENISA, 2004

Contingencies to make the outcomes more or less satisfactory are typically built into project plans[43]. There are at least 16 methods of risk assessment[44] but the emphasis seems to be on opening up the issues rather than matching them with a method of treatment.

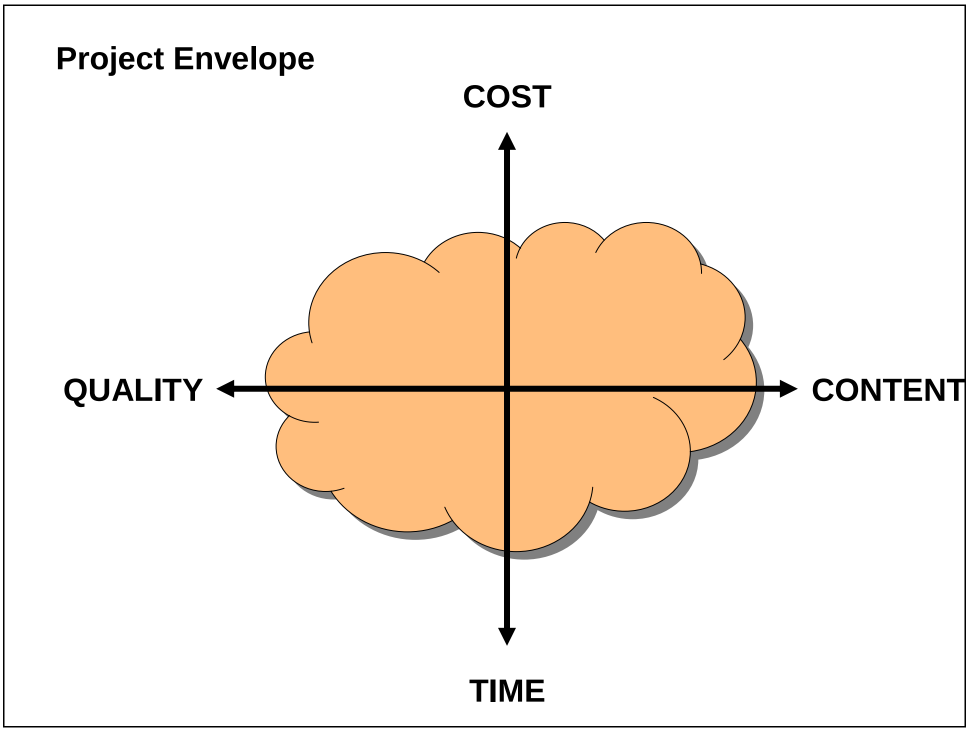


Figure 2: The project envelope

Risks are associated with one or more certain or uncertain events (a single occurrence or a series of occurrences of a particular set of circumstances) which have a likelihood or probability (extent to which an event is likely to occur) of happening. Events have consequences (outcomes) can range from positive to negative. There can be more than one consequence from one event. However, consequences are always negative for safety aspects. Consequences can be expressed qualitatively or quantitatively.[45]

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[43] BS 6079-3 *Project management – Part 3: Guide to the management of business related project risk*, British Standards Institution, 2000

[44] BS 6079-3 *Project management – Part 3: Guide to the management of business related project risk*, British Standards Institution, 2000

[45] PD ISO/IEC Guide 73, *Risk Management – Vocabulary – Guidelines for use in standards*, British Standards Institution, 2002

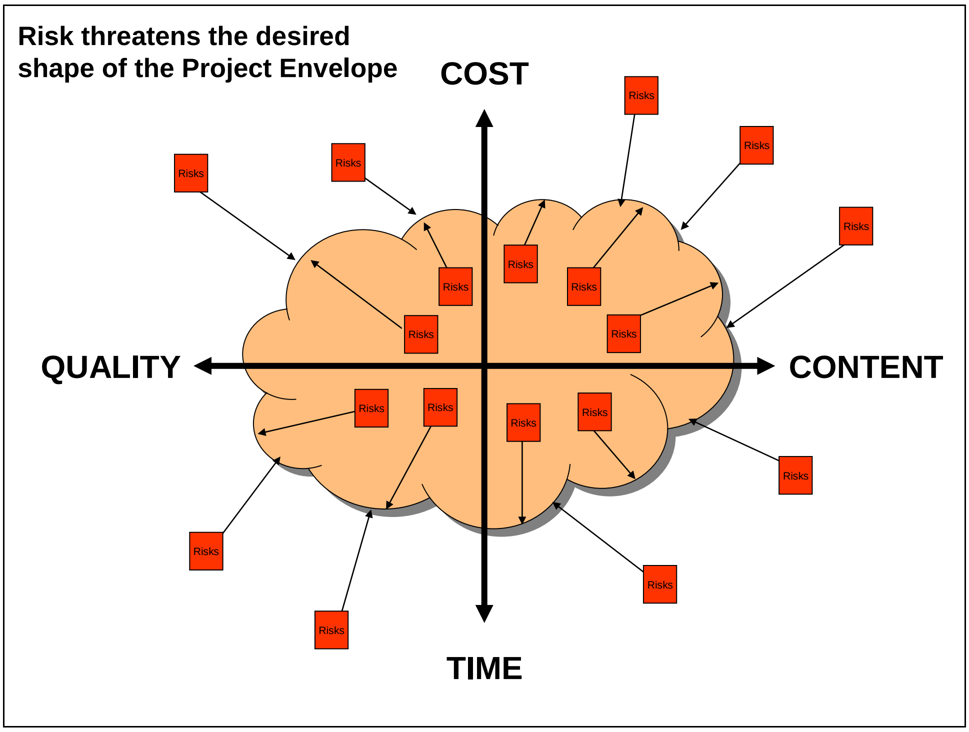


Figure 3: Risk threatens the desired shape of the Project Envelope

Risks can be known (if not explicitly as risks, at least as concerns by at least one person), unknown (in so far as they could be found with the appropriate weltanschauung), or unknowable (the truly emergent risks that no one could reasonably foresee)[46]. Standards provide an anchor for all the change that must be managed in an agile business. They are a toolbox which is too often rejected unopened, and the tools needed to fix a solution overlooked as proverbial ‘wheels’ are reinvented. Take this ISO/IEC 27002 and pick and mix the controls for your project and security plans, and identify (for that's covered in the standard) what they should deliver. With planned, project activities, you can categorise and prioritise them and allocate them to people with the most appropriate sets of skills, responsibility and authority and so be tough on both risk and the causes of risk[47]

1.5.3.3. Security policy

This section drives the creation of the core of the ISMS documentation. It mandates the creation of an information security policy, and specifies a minimum content: a definition of information security as it applies to the organisation, and a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation. It also mandates a review process that we’ll covered in increasing detail below. It sets out an overarching goal of business continuity.

1.5.3.4. Organisation of Information Security

Successfully managing an ISMS requires key staff to take ownership of various responsibilities, and management structures to be in place to support them. This section sets down the specification for allocating responsibilities for a range of tasks. It also specifies the need to have a source of expert advice which may mean external consultants, membership of an external forum, or making an in-house expert available. The need for ongoing independent review is stated in this context as well. Lastly, this section addresses the relationship with third parties – such as contractors and outsourcing

[46] Marvin J. Carr, Suresh L. Konda, et al., *Taxonomy-Based Risk Identification*, Software Engineering Institute, June 2003

[47] cf. risk and the causes of risk with ‘crime and the causes of crime’, Labour Party Manifesto, 1997

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

companies – and the extra security framework that needs to be in place before these parties are granted access to the organisation's information. The standard provides a security-centric checklist for service level agreements (SLAs) that complements the contents recommended by the IT service management standard ISO/IEC 20000[48]. The explicit and implicit interconnectedness of information systems and their outcomes and potential misuse is also covered by the need to have a measured response when authorities such as the police may need to be contacted.

1.5.3.5. Asset management

Knowing what you are protecting is a critical part of building an ISMS. You will not want to use controls from ISO/IEC 27002 inappropriately. So, this part of the standard deals with the need for a complete inventory of assets, showing ownership, location, and importance. The loss or inaccessibility of any these assets may have an impact on business continuity. Examples of asset categories may be:

- Information assets – such as databases, documentation, procedures, backups.
- Software assets – operating systems, off-the-shelf applications, bespoke applications, utilities and tools[49].
- Physical assets – computers (processors, monitors), communications equipment (routers, modems, telephone exchanges), media (tapes, disks), other equipment (uninterruptible power supplies, for example), furniture, cabinets and accommodation.
- Services – heating, lighting, air-conditioning, electricity, as well as communication services and any outsourced computing services
- People – such as specially qualified staff who are retained for knowledge and experience. Business continuity is not achieved by the unqualified working 'by numbers'
- Intangible assets like good will and reputation

This section also covers the classification and protective labelling of assets, and associated procedures for copying, transmitting, storing and destroying the information assets – information has a lifecycle and the need for confidentiality will vary throughout it.

Just knowing what you have is not enough. It must also be clear as to the acceptable uses to which each asset may be put. This needs to cover all who may use the assets so remember temporary and contract staff too.

1.5.3.6. Human Resources security

Controlling computers can be comparatively easy. With the right configuration and tools, and good administration, computers will do exactly as they are told (in most cases). The same cannot be said for people who, either accidentally or deliberately, constitute the largest single threat to any information system. This section deals with all issues relating to the users of the information system. It addresses the responsibilities that they must bear, and how they should be motivated to fulfil their responsibilities by awareness and training. All this need to be governed by explicit terms and conditions of employment, supported by the need to ensure that the disciplinary procedures give the organisation the statutory powers to take action against internal miscreants.

The standard gives structure to the controls that need to be consider when staff are recruited, move around the organisation to areas that need greater or less degrees of confidentiality, and eventually move on (of their own accord or otherwise) and the handing back of assets they may have used relatively freely for considerable time. Vetting staff – permanent, contract, or temporary is not something to be taken lightly with the threat of fraudsters seeking to enter employment with longer

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[48] ISO/IEC 20000 is the measure of the implementation of the appropriate best practice from the IT Infrastructure Library (ITIL).

[49] Software asset management is an art in itself and warrants its own best practice guidance – see ISO/IEC 19770

term nefarious ideas. Again, standards give some structure to managing this risk and advice is given in BS 7898, *Security screening of individuals employed in a security environment — Code of practice*.

1.5.3.7. Physical and environmental security

Secure computing always places a primary emphasis on the network as the prime entry mechanism for any illicit activity or attacks; not unfairly, since the vast majority of potential attackers can only access their target systems across networks. However, the physical security surrounding systems is just as significant. Network-borne attacks may be thwarted with comparative ease, but an attacker with physical access to a server is almost guaranteed a successful intrusion. This section of the standard sets down requirements for secure areas, the controls required to enter such areas, and the precautions to be taken when inside one.

With so much mobile equipment, don't forget the implications of staff on the move, and don't let your public-access areas become a conduit for theft or other intrusion.

Environmental security covers such issues as protection against power cuts, flooding, and electrical surges – all of which can interrupt the availability of an information system. Planning ahead to deal with these factors is essential; without the appropriate safety nets in place, recovery from any of these disasters is not trivial.

1.5.3.8. Communications and operations management

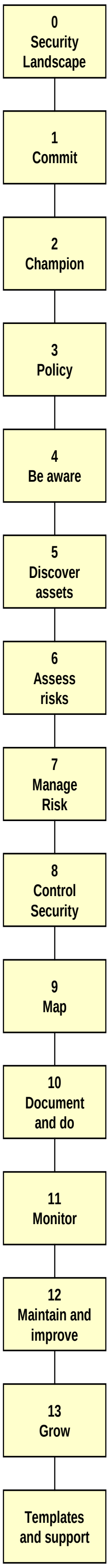
The scope of this section is one of the widest – from the segregation of duties to protect against fraud to the importance of guarding against malicious code (such as viruses, worms and Trojans). Don't be surprised that the section is so large. Bringing an information system up to any given standard is straightforward compared to the complexities of keeping it there. However, the standard breaks it down into tasks that can be prioritised according to your assessment of the risks.

This section also covers processes to secure different elements of e-commerce change control, incident management, outsourcing to third parties[50], the need for separate test facilities, managing risks to confidentiality or disclosure when exchanging information, back-ups, the security of e-mail, and the disposal of media. Monitor your systems – such as the maintenance of logs – and the review of what they may show you – is here. There was a time when synchronizing clocks was key for share traders and a convenience for others. Now with the proliferation of 24-hour e-commerce transactions and the unfortunate need for unambiguous forensics trails, there can be few to whom this control will not apply.

1.5.3.9. Access control

This is a strict but pragmatic view of enabling business needs. At the simplest level, the requirements of the standard touch upon the need for a sound user management system, for the creation and deletion of accounts, and the characteristics required by their passwords in terms of length, complexity and lifetime. Authentication is separated from authorisation so that privileges will be managed properly. Best practice dictates two key requirements in this field: firstly, that by default, permission to access a resource be denied – so that it needs to be specifically permitted when such access is genuinely required; and secondly that the scope of such access, when granted, must be limited only to those resources which are actually needed. The standard's requirements for network, operating system and application access control reiterate these requirements. A component of security is availability and this section provides the framework for the safest realisation of connecting users through fixed, mobile, and teleworking arrangements.

Detection of access control abuse is covered – with emphasis on the importance of scaling this correctly so that such illicit access may be identified; and hence the need to find a balance between



[50] So ISO/IEC 20000 for IT Service Level Management is useful here too.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

recording so little information that the activity goes unnoticed, and so much information that the activity becomes impossible to spot.

And just as there are rules for granting access, there are a set of counter rules about taking access away.

1.5.3.10. Information systems acquisition, development and maintenance

You can't separate security from quality. Retrofitting security to systems and their applications – particularly bespoke applications, either developed or integrated in-house – is far more difficult, disruptive and complicated than simply building it in from the outset. This section covers the factors that need to be considered throughout the lifecycle[51] of a system, to prevent exploitation through that system[52]. Data entering the application must be validated; messages to or from other systems must be demonstrably authentic and not open to repudiation. Of course, this raises the topic of digital signatures and the accompanying cryptography and certificates. Staying within the boundaries of the data protection act is built in here with the caveats of test data and processing information with integrity.

The Trustworthy Software Framework – set to become PAS 754 – establishes a pattern for systems to be developed and maintained with the qualities of trustworthiness which are shown in Figure 4. *See 1.5.6 The Trustworthy Software Framework (TSF).* Security is a clearly defined element of this which may be achieved with controls to achieve the three action to protect, operate, and self-preserve:

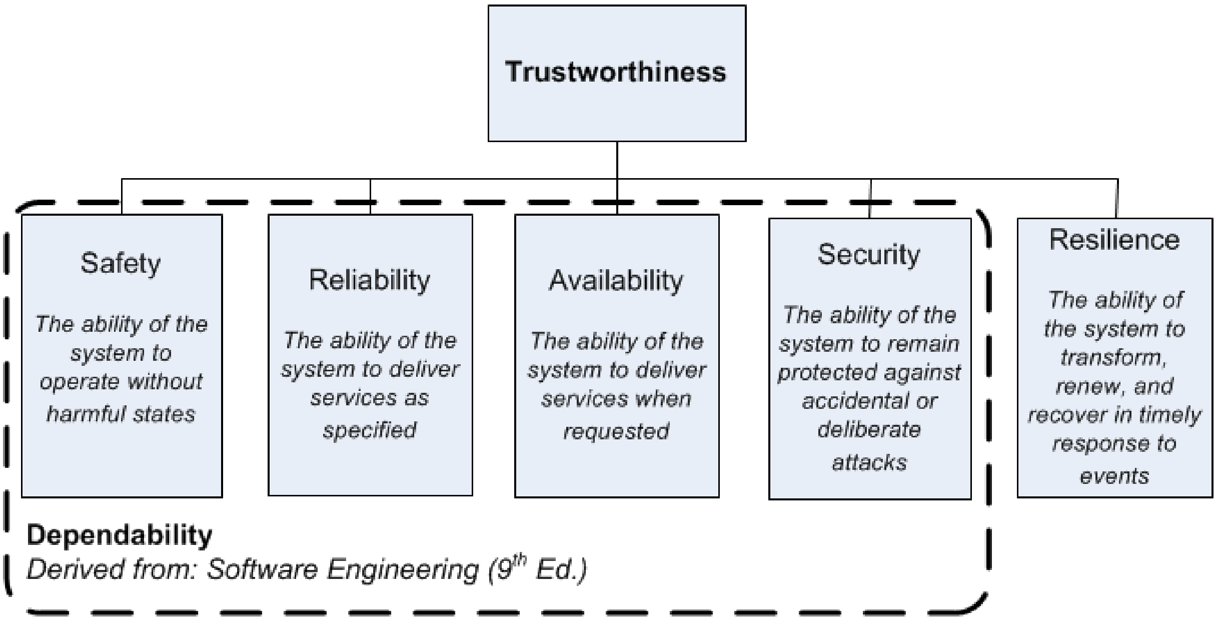

Trustworthiness
Safety
The ability of the system to operate without harmful states
Reliability
The ability of the system to deliver services as specified
Availability
The ability of the system to deliver services when requested
Security
The ability of the system to remain protected against accidental or deliberate attacks
Resilience
The ability of the system to transform, renew, and recover in timely response to events
Dependability
Derived from: Software Engineering (9th Ed.)

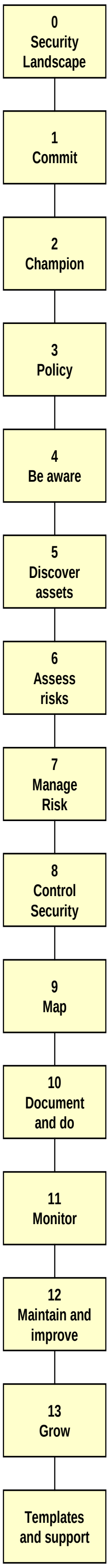
Figure 4: Attributes of trustworthy technology

These objectives need to be applied to operating systems and applications, cloud computing, smartphones and tablets, consumerisation and bring-your-own network/device/'app' in business, and the way that these are organised such as-a-service computing utilities, commoditisation in previously closed architectures, system consolidation, and virtualisation. In addition, software development itself is changing thanks to factors such as the adoption of open source models for sourcing software, the growth of multi-core processor technologies, a blurring of the boundaries between software and

[51] See ISO 15288 for Information System lifecycles

[52] The criteria for testing systems – the product view of security rather than the processes of ISO/IEC 27001 – are set out in the parts of ISO/IEC 15408 *Security Techniques – Evaluation Criteria for IT Security* (often referred to as the Common Criteria).

hardware, the adoption of approaches such as agile and rapid application development, and the growth in small-scale software development[53].



1.5.3.11. Information security incident management

The uninitiated expect that standards must instil perfection and therefore a security standard must make all secure. This is clearly an example of at best a problem of semiotics and at worst poorly managed expectations. There will be security incidents. Some of them may even be serious. However the realism of ISO/IEC 27001 is that it does not expect you to have second sight and an infinite budget to act on your visions but rather that you have made all reasonable steps to manage the risk and assure business continuity[54]. The issue is to make sure that you can differentiate between events such as the user problems of forgotten passwords, and the incidents of deliberate compromise attempts. To put it into the words of one industry leader, how do you keep the residual footprints of incidents to a minimum? This is the 'catch all' and a vital source information about the effectiveness of your ISMS and how you may need to develop it.

1.5.3.12. Business continuity management[55]

Related, in part, to the section covering environmental security, this section provides a framework for creating plans that will – in the event of disaster or failure – allow business operations to be maintained, or recovered in the shortest possible time. When the computer goes down, the business can go down with it. What about desk space and a telephone in the event of a fire? Business continuity plans – tested plans to make sure that you can reload a back-up tape, get in touch with key personnel who are off site etc. – are the foundation to keeping business going through minor interruptions through major disasters. They are the strategy and guidance for you to continue to satisfy expectations.

1.5.3.13. Compliance

The stated objective of this section is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. Information about various items of legislation is detailed, in a generic manner that does not relate to any particular country or territory's legal system or code. Matters such as intellectual property and licensing, data protection, cryptography, and collection of evidence (so we need to be aware of the processes for successful computer forensics) are included in the scope. There is not really a branch of special IT laws but rather legislation that is relevant in the deployment of IT. This is where you bring in your own scrutiny of audits – using tools where possible – in a framework that does not allow the audit process to create a weakness in the ISMS.

This needs to include an understanding and achievement of a state of forensic readiness[56]:

(1) Define the business scenarios that require digital evidence.

(2) Identify available sources and different types of potential evidence.

(3) Determine the evidence collection requirement.

(4) Establish a capability for securely gathering legally admissible evidence to meet the requirement.

(5) Establish a policy for secure storage and handling of potential evidence.

(6) Ensure monitoring is targeted to detect and deter major incidents.

[53] http://www.uk-tsi.org.uk/

[54] A practical manual for information security incident management is ISO/IEC 27035 (which replaced ISO/IEC TR 18044).

[55] A best-practice framework for Business Continuity is set out in ISO 22301.

[56] Rowlingson, Robert, *A Ten Step Process for Forensic Readiness*, International Journal of Digital Evidence Winter 2004, Volume 2, Issue 3

(7) Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.

(8) Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.

(9) Document an evidence-based case describing the incident and its impact.

(10) Ensure legal review to facilitate action in response to the incident.

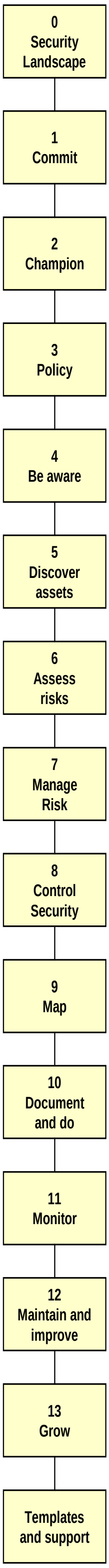
1.5.4. Other standards and futurology . . .

We looked above how the knowledge from a survey drove forward the awareness of a need to do something about information security. But in standards land there is often a 'knowledge base' of related information that is waiting for its time to come. This means that you have to have the carpe diem attitude of using the guidance to hand but have the foresight to keep an eye out for new help that comes along as standards work their way along the road of continuous improvement.

The ISO/IEC 27002 standard that everyone has been getting excited over in 2005 will be joined by the internalisation and improvement of its counterpart, the auditable ISO/IEC 27001 (that was BS 7799 Part 2). It is was BS 7799 Part 2 that first defined how you can have a system that establishes which of the controls you need to select from the catalogue (or strictly speaking the code of practice) which was born as BS 7799 Part 1 and became ISO/IEC 17799. It's the part which makes the standard relevant to any size or complexity of organisation. All of these numbers are going to settle down in a year or two, but momentarily let's consider something that may become, at least euphemistically, BS 7799 Part 3. This is going to be the risk management recommendations that we alluded to above. It will knit all the rest of the standards together more harmoniously by driving home the idea that secure enough is secure enough; it's the management of the risks that help you make that assessment of what risks are acceptable so that you can come to that 'secure enough' decision (all sorted out in stage 7 of the implementation plan that is the focus of this best practice guide).

The ultimate structure of what started as BS 7799, became ISO/IEC 17799, will be the complete ISO/IEC 27000[57] series. This will comprise (at least!):

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27001 — Information security management systems — Requirements.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC 27010 — Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

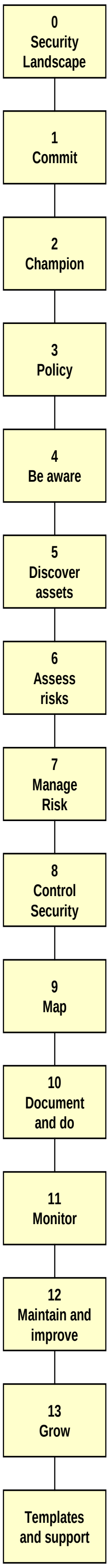


[57] No hocus pocus in the numbering. BS 7799 was just the number allocated to the original code of practice. It couldn't become ISO 7799 because that number had been allocated, so the '1' was prefixed. The subcommittee of the Joint Technical Committee of the International Standards Organisation and the International Electrotechnical Commission that deals with keeping ISO/IEC 27001, ISO/IEC 17799 et al. up to date is 'SC27'.

- ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 — Information security governance
- ISO/IEC 27017 — Information security management for cloud systems
- ISO/IEC 27018 — Data protection for cloud systems
- ISO/IEC 27019 — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO/IEC 27031 — Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27032 — Guideline for cybersecurity
- ISO/IEC 27033 — IT network security
- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27033-2 — Guidelines for the design and implementation of network security
- ISO/IEC 27033-3:2010 — Reference networking scenarios - Threats, design techniques and control issues
- ISO/IEC 27034 — Guideline for application security
- ISO/IEC 27035 — Security incident management
- ISO/IEC 27036 — Guidelines for security in supplier relationships
- ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence
- ISO/IEC 27038 — Specification for redaction of digital documents
- ISO/IEC 27039 — Intrusion detection and protection systems
- ISO/IEC 27040 — Guideline on storage security
- ISO/IEC 27041 — Assurance for digital evidence investigation methods
- ISO/IEC 27042 — Analysis and interpretation of digital evidence
- ISO/IEC 27043 — Digital evidence investigation principles and processes
- ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC TR 27015 — Information security management guidelines for financial services
- ISO 27799 — Information security management in health using ISO/IEC 27002

So we should be asking who's certificated to ISO/IEC 27001.

We noted above how ISO/IEC 27002 has a clause dedicated to the management of information security incidents and events. It's a big enough topic to warrant its own standard so the reading list needs ISO/IEC 27035 adding to it to cover 'Information security management'. This gives a comprehensive approach to the corrective and preventive action surrounding information security incidents and so has an affinity for the quality management processes of the ISO 9001 standard for quality systems. To be cost effective, integrate management systems so that the same communications channels that you use to deal with customer feedback can be used to report security incidents. Both need an appropriate response in the short term and longer term root cause analysis and improvement. Similarly, if incidents are not being dealt with in a timely manner the escalation routes can also be shared.



Some organisations will have a better attitude to building in information security than others and this approach can be benchmarked using the ‘Systems Security Engineering Capability Model’ that is recorded in ISO 21827.

On the whole, the standards that we have discussed – and especially core information security management system standard (BS 7799 Part 2 becoming ISO/IEC 27001) – are **process standards**. You cannot stamp a product’s security worthiness with a certificate to this standard; however it is meritorious if it’s been created within an information security management system that has been certificated to the process standard by an accredited third party. Products should be the target of evaluation under the requirements of the standard ISO/IEC 15408 – the Common Criteria for IT Security Evaluation. This is the environment in which you really can find out whether it does what it says on the tin.

It is also worth clearing up a small but significant point of order here and that is the relationship with ISO/IEC 20000 (originally BS 15000), the standard for IT service level management. This standard set out the controls and service arrangement for outsourcing either to a genuine third party or as is often the case) an in-house IT department. It’s incredibly useful for defining the contents of service level agreements (SLAs) and is enhanced by the guidance for specifying security requirements in SLAs in ISO/IEC 27002. Both outsourcing or the in-house scenarios have in common the customer, the supplier and a need for coherent, mutually agreeable collaboration and cooperation Not surprising is it that security requirements are referenced and the standard clearly notes that an information security management system of the BS 7799 standard (sic!) – and that means a relevant, encompassing scope - will meet the requirements of ISO/IEC 20000. It does not mean, as some have come to misinterpret, that an organisation that meets the requirements of ISO/IEC 20000 doesn’t need ISO/IEC 27002/ISO/IEC 27001, nor vice versa.

1.5.5. Information Assurance for Small and Medium Enterprises Standard (2013) – IASME

A standard that was developed to support the information security of SMEs but has matured into a cyber security standard and is now applicable to all sizes of organisation in all sectors of the economy.

A company that complies with the IASME Standard will have the appropriate control set implemented to prevent compromise. Protective measures are selected and implemented according to risk of (for example) low-end compromise through technical and human-vector attacks on organisational data and devices, personal devices, social engineered attacks, risks associated with cloud architecture and services and malware. This list is indicative of low-end methods of compromise and is not exhaustive. The IASME baseline establishes the foundation for protection against more sophisticated threats as they migrate through the supply chain.

Because the cyber threat vectors to organisational confidentiality, integrity and availability are diverse and pervasive, protection must be integrated and holistic. The IASME Standard therefore specifies physical, procedural and technical controls to prevent, detect, and recover from information compromise arising from multiple threat vectors, which are suitable for organisations of all sizes.

IASME control sets may be mapped to any sub or super set of NIST 800-50, BS ISO/IEC 27002, SANS 20 etc. and hence IASME provides commensurate protection against the risks these other standards have been formulated for.

Although originally developed for small companies, it is possible to scale the Standard to much larger organisations by managing the scope(s) of the assessment. This will be achieved by a two stage risk profiling method which offers simple procedural controls to highly granular controls depending on the required level of risk management. Over the next six months the methodology to apply IASME to companies of any size will be developed, tested and launched.

The IASME Standard has an assessment process which is centrally controlled and moderated by The IASME Consortium. The IASME certification process is designed and implemented to meet the

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

expectations of the UK Accreditation Service (UKAS). Moderation assures the consistent quality and uniform application of the IASME standard by an SME.

An IASME assessment looks at the governance of cyber security across the legal entity and dependencies upon other organisations.

IASME assessors must pass a mandatory training programme including an intensive 1-day course . IASME assessors passing the training become accredited by successfully (as judged by an IASME moderator) completing at least two supervised certifications. Training is designed to be accredited by Continued Professional Development (CPD) programmes.

Assessors are assigned to companies with which they have no commercial relationship . IASME assessors make recommendations but only IASME Moderators certificate.

Assessors pay fees for the course and an annual licence to defray the cost of continuing accreditation. IASME's documentary items for candidate companies and the distributed assessment network controls travel time, contact time, and overheads so reducing the SME's fees. Fees are weighted to the number of sites and employees an SME has in keeping with other national schemes.

The SME market is notoriously price sensitive. The market itself will continue to keep prices down. If the cost of assessment is too high then SMEs will simply not buy.

The Standard is aligned to the internationally recognised ISO/IEC BS 27 family of standards, ICO Principles and other HMG guidance. It also includes elements of NIST (USA), ENISA (EU) and other relevant guidance. A document published on the website shows details of how the IASME standard aligns with the ISO/IEC 27001 standard.

The IASME standard has specifically been written to apply internationally. It refers to local laws and regulations rather than assuming it is used only in the UK.. Indeed, partnerships with international organisations are currently being explored with the aim of exporting this standard internationally. This process is expected to occur through large commercial organisations rolling the IASME specifications out to its SME suppliers around the world.

This potential export has come about because global organisations can see the benefit of specifying one minimum cyber hygiene standard to all their supply chain, regardless of which country they may be located.

IASME is a risk-based methodology for cyber security and therefore manages risk as a priority, in particular those posed for low-end methods of compromise. The early consideration of risk makes a direct connection between the level of risk and the controls deemed necessary to reduce that risk to an acceptable level and manage the residual footprint

The IASME Standard maps the full spectrum of controls contained in ISO/IEC BS27002 and the other referenced guidance, albeit expressed in more business-friendly terms and is constantly reviewed to keep abreast of contemporary threats (including specific 'bring your own device - BYOD and cloud computing related threat vectors). In addition, the Standard contains controls for the new, rapidly evolving threat landscape derived from our own and other reputable threat analyses so that it remains up to date.

The modular approach to risk has created a framework where future development of the standard may result in the introduction of controls to address high end threats too. These are entirely assessable under the current IASME framework.

The Standard includes the full spectrum of physical, personnel and technical controls as shown in this overview:

- ***Organisation***
  Manage information resources within the organisation and in the organisation's relations with partners.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

- ***Risk***
  Understand and manage the risk to your business information.
- ***Policy and Compliance***
  Establish legal and regulatory requirements, management direction and communications. Know what is required and monitor compliance
- ***Assets***
  Know the value of your information assets, and acquire and dispose of them securely.
- ***Planning***
  Build security and privacy in at the start; make sure you have the right-sized information systems.
- ***Access***
  Control who and what can access your information.
- ***People***
  Know your people and educate them in business security.
- ***Physical and Environmental***
  Protect your information assets from physical and environmental harm.
- ***Disruption***
  Defend your information from hostile attack and be ready to recover from the effects.
- ***Operations***
  Manage and monitor your information systems effectively.
- ***Incident management***
  Ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons.
- ***Continuity***
  Make sure you can recover quickly from partial or total loss of key information assets.

1.5.6. The Trustworthy Software Framework (TSF)

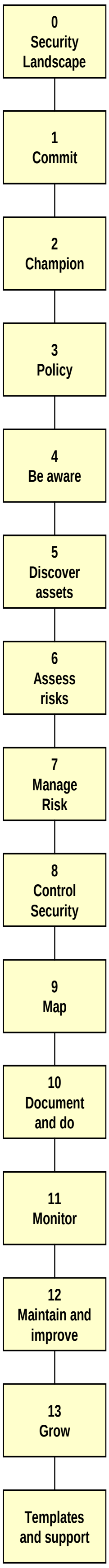
TSF is an upcoming standard of activities necessary to assure that software is developed, operated, and maintained so that it has and retains the follow attributes in acceptable measures:

- **Safety -** the ability of the system to operate without harmful states
- **Reliability -** the ability of the system to deliver services as specified
- **Availability -** the ability of the system to deliver services when requested
- **Resilience -** the ability of the system to transform, renew, and recover in timely response to events
- **Security -** the ability of the system to remain protected against accidental or deliberate attacks

TSF is maintained by the Trusted Software Initiative of de Montfort University and is a public-private platform for enhancing the overall software and systems culture, with the objective that all software should become designed, implemented and maintained in a secure, dependable and resilient manner.

Requirements for Trustworthy Software can arise from:

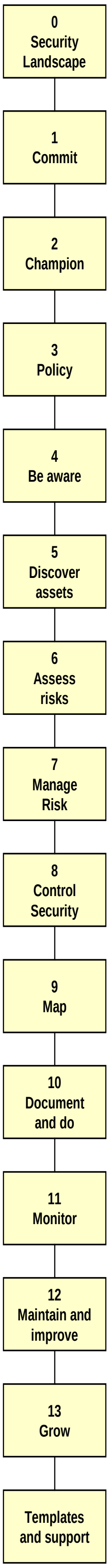
- Explicit (Functional) Requirement for Trustworthiness
- Implicit (Non Functional) Requirement (NFR) for Trustworthiness, which may be:
  - Direct NFR for software under consideration
  - As Collateral NFR from other software in environment



Requirements cover whole ICT domain and activities (specification, realisation and use). Assurance requirements range from Due Diligence (all software) to comprehensive. Many of concepts and practices needed for software Security / Dependability / Resilience have existed in specialist domains for many years. They must be ‘baked in’ to all software, recognising that implementations may vary with audiences and functional/assurance requirements.

Beneficiaries of trustworthy software will include:

- **Demand-side**
    - A *de facto* or *de jure* expression of specification, providing risk reduction
    - A target for compliance
- **Supply-side**
    - A level playing field, with improved business opportunities
    - Avoidance of nugatory effort, and reduced cost of doing business
    - A target for compliance
- **Corpus-production side**
    - *De facto* or *de jure* repository of knowledge
    - A target for compliance



2. How to Develop and Improve an ISMS

2.1. What is an Information Security Management System (ISMS)?

2.1.1. The ISMS

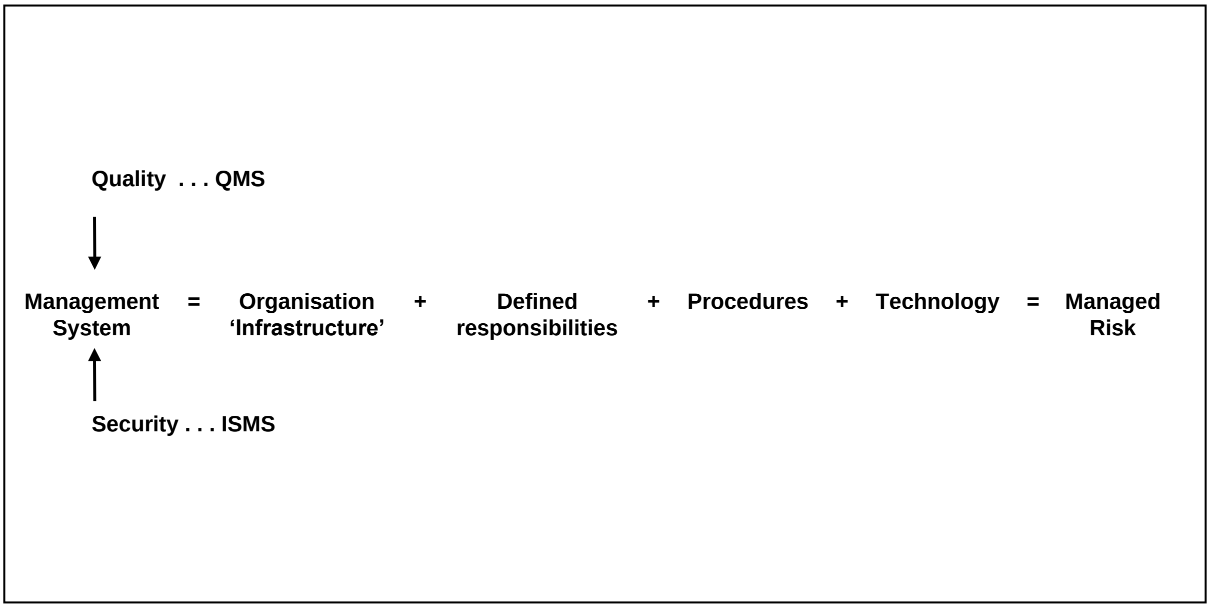
An ISMS is the implementation of a documented set of policies, processes and procedures that pin down the general requirements of the code of practice to the individual nature of the organisation. Targets are set, controls are put in place to meet them, and measurements are made to confirm that risks to information assets are being contained within an acceptable range or initiate improvements to make it so.

At the simplest level we are talking about the interaction of people, technology and processes within an organisation. First and foremost in the ISMS, which to the merit of many organisations is just the 'Management System', is the organisation itself. This means how it is arranged in terms of buildings and depots, shops and offices, executive and non-executive boards, all levels of management, project teams, sales force, site services, and so on.

The next part of the model, which will vary from size and 'maturity' of the organisation, is a combination of the defined responsibilities (which may manifest themselves in job descriptions) and the procedures for doing whatever it is the organisation does. The latter may be a mature set of instructions that are followed by all staff from switchboard to boardroom. They may be a rather ad hoc affair of success (or otherwise) based on ‘Arthur who's been here for 25 years and has always done it this way’.

Then there is the technology employed to process materials and information that is too often perceived as the management system because of its tangibility. It merely comprises the tools and as you define your ISMS you must consider whether you need all the tools for the job.

Figure 5: The components of a business management system



2.1.2. Specifying, implementing and maintaining a security management system

This process is designed to provide a managed framework to the implementation of processes and tools required for a management system that complies with ISO/IEC 27001. In its first iteration, it will not specify the all the 'how to's' so as not to complicate the framework. The selection and implementation of appropriate tools for security management such as access controls, authentication systems, vulnerability scanners and so on will be added as the methodology develops. As with the

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

intention of ISO/IEC 27001, the methodology is designed to deliver a security management system that is fit for the purpose for which it is intended. Not all the ISO/IEC 27002 controls will be appropriate to all organisations and different organisations will need to apply the controls at different levels.

The ISMS is a set of documented processes and procedures, realised by staff and other stakeholders, that specify the organisation's approach to information security, and show its compliance to ISO/IEC 27001. The core of the documentation is a triad of documents:

- The **security policy**
  A high-level document setting out the aims and objectives of the ISMS, and affirming the management commitment to information security
- The **statement of controls**
  A definition of the detailed policies and resources (such as personnel), activities and tools that will be in place to secure the information assets
- The **statement of applicability**
  A route map of which security control is applied, where it is applied, and the rationalisation for excluding any controls. This is benchmarked against ISO/IEC 27001.

But these core documents alone cannot provide any meaningful protection because they exist at too high a level. Strategically they are vital, but they will be of limited use to those involved in the implementation and administration of the organisation's information systems. They must be supported by further layers of documentation. Usually these layers will be made up of two types of document:

- **Standards**: Which state the 'dos and don'ts' required of the systems, the baselines specifying their minimum configurations, and the recommended levels to which the systems should aspire where possible. These documents answer the question: 'what must be done?'; and
- **Procedures**: The detailed instructions for the implementation of the standards. These documents answer the question: 'How should we do it?'

The security policy and its supporting documents provide the underlying structure of the ISMS around which controls need to be put into place. It is necessary, first, to define the scope of the ISMS – to decide in organisational, physical, geographical and logical terms which systems are covered by the policy. The ISMS itself is created by implementing controls – where appropriate (and this is usually decided by a risk analysis) – on the systems deemed to be in scope. An ISO/IEC 27001 compliant ISMS would use the catalogue of controls that are provided in ISO/IEC 27002.

The story does not end there. An ISMS is partly about analysing an organisation's requirements and putting the appropriate controls in place; but it is also about maintaining the currency of the controls and ensuring that they are respected into the future.

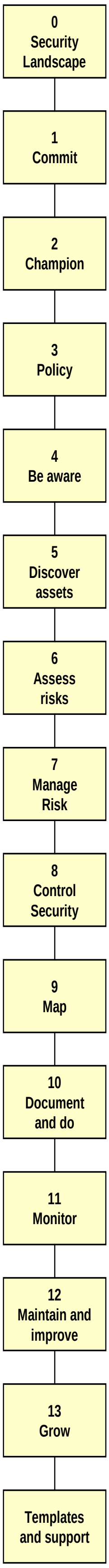
In summary, the most important letter in the acronym ISMS is the second 'S'. An ISMS is not a set of documents; nor is it a set of procedures; nor a tool. It is a **system**: a combination of all the above, and many other factors – such as well trained staff.

2.2. What's in this method?

This chapter is the main component of this Guide and is presented in the most practical way possible, without doing the work for you. You can't buy a management system off the shelf. Well perhaps you can, but it won't be right for your business, it will add operational cost and reduce the benefits that standards experts have distilled into the ISO/IEC 27001 standard. You might just manage to get a bought-in system certificated but that will be more luck than design and just wait until you try to run your business and maintain a parallel management system.

Here we focus on:

- Defining the information security management system (ISMS)



- A framework method for constructing, developing, and maintaining an ISMS

By following a classic ‘Deming’ model:

- **Plan**: Look at your assets and work out what needs to be done to protect them.
- **Do**: Implement the processes – run your business!
- **Check**: Monitor and measure processes and product against policies, objectives and requirements for the product - document and report the results.
- **Act**: Take actions to continually improve process performance - feed it back to the planning.

Using this method you will identify all the good things that you have in place already, build on successes, and learn from failures. You may have the expertise to pick this method up and run with it but you may need some expert help; see: *Who is a Security Expert?* below.

2.3. Structure of the method

The methodology is presented as a programme of work comprising modular activities that an organisation can pick up and use to create a project plan. Indeed, it is probably essential to educate organisations that the development and implementation of a security management system must be treated as a project, duly prioritised and resourced in the same way as any other mission critical activity should be.

The stages and activities although modular, may not remain discrete or sequential. It is envisaged that as the experience of the organisation grows, and the effectiveness of the management system develops, stages will be revisited. For example, the statement of controls (or detailed security policy) is likely to be revisited many times in the early drafting and then subject to a programme of continuous refinement and improvement. The stages comprise:

(1) Persuade top management of the need to act on security issues.

(2) Appoint security champions to represent all activities

(3) Compose and agree your high level security policy.

(4) Create security awareness: train and educate staff.

(5) Identify and classify the assets.

(6) Assess the risks to your information assets.

(7) Plan how to reduce risk to an acceptable level.

(8) Establish pragmatic security policies.

(9) Map out where your security controls should be.

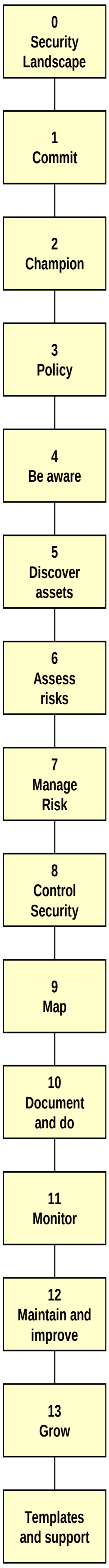
(10) Write and implement your system security plans, processes, and procedures.

(11) Monitor and review the ISMS performance.

(12) Maintain the ISMS and ensure continuous improvement.

(13) Extending the scope of the security management system.

Each stage is covered separately in the main body of this best practice guide, but here they are in summary[58]:

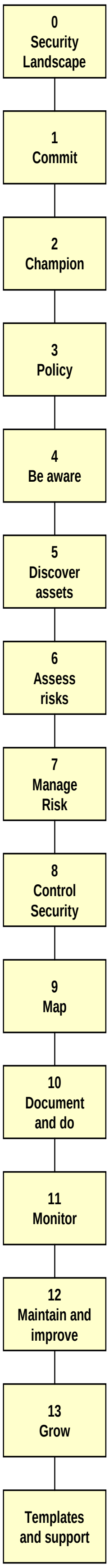


[58] Adapted from *MANAGING RISK: Technology and Communications* Jonathan Armstrong, Mark Rhys-Jones, Daniel Dresner, ISBN: 0-7545-2468-x, BUTTERWORTH HEINEMANN

2.3.1. Persuade top management of the need to act on security issues

No matter where an idea comes from – staff, customers or the company board – it must carry the approval of top management to ensure that it receives the resources needed and remains at the right level in the priorities list. This stage collects any issues identified to date, presents the business case for the implementation of the ISMS and hands the baton to those who will see it through the forthcoming stages defined below.

This is a vital (and sometimes overlooked) strategic requirement for the implementation of an effective information security management system. Securing such support can be difficult, as top management is guaranteed to be occupied with day-to-day pressures; but finding an 'information security champion' at a high level can dramatically reduce operational resistance to the inevitable changes that a formal ISMS will bring, and therefore the effectiveness of the system can be greatly enhanced.



2.3.2. Appoint security champions to represent all activities

After you have issued the security policy statement, establish structure for managing security within your organisation. This is necessary to ensure the organisation's involvement in identifying and implementing various security measures.

The implementation of the ISMS will need the buy-in from the whole organisation, not just initially, but also when threats are identified or incidents occur. You will need a mechanism whereby you can collect a holistic view of the impact of security issues and a channel for disseminating the information and actions. You need a team of information security champions that represents the makeup of the organisation and who will coordinate the implementation and maintenance of the controls that are selected.

You may decide to implement or expand your ISMS in phases. This has the challenge of secured parts of the organisations having to interact with other that may be unsecured. Manage these relationships with service level agreements (SLAs).

Deperimiterisation has its effect here. An organisation needs to concern itself not only with its users, but also its supply chain, those its thrall, and the social and regulatory regime within which it operates. Make sure that representation is wide enough to manage all the interfaces with your 'extended' business.

2.3.3. Compose and agree your high level security policy

This is where the information security champions works with top management to set the scope of the management system and high-level security policy. Policy documents form the core of any ISMS. They formally set down the requirements of the system, and provide the mandate from the top of the organisation that ensures the ISMS can be enforced operationally. All questions of security lead back to this policy and it must be regularly reviewed by top management for its effective implementation and continuing relevance to the business that the ISMS sets out to protect.

2.3.4. Create security awareness: train and educate staff

Information security will involve every member of the organisation be they responsible for designing products, delivering services, or maintaining the areas in which the designers work. Information security touches the whole organisation whether they are ICT users or not. Each person has capability of sabotaging the information security through ignorance, or with malicious intent. A careless comment about a customer may do expensive or irredeemable damage to the organisation's brand.

Education and training is needed to explain each individual's role in maintaining the information security and his/her responsibilities towards every information asset that they handle or have access to. Education and training should be comprehensive and adequate to ensure that each person clearly understands the security policies of the organisation, various security risks and threats, the processes and procedures to be followed, and finally consequences of not abiding by the security procedures.

2.3.5. Identify and classify the assets

It is difficult to protect what you do not know that you have. And you can't deal consistently with things whose value you do not understand. The purpose of this phase is to identify the organisation's information assets which may vary from computers, databases, or printed and hand-written documents and know something about these assets. This is also where you broaden the championship of security and make sure that each asset can be attributed to an owner. Once you know something about what you have, the information security champions can work with the asset owners to make sensible decisions about the acceptable levels of risk and the level of protection required to keep public information accessible and private information available to those who need to know.

2.3.6. Assess the risks to your information assets

Once you have a comprehensive list of all the critical assets whose failure could impact on the business and the C-I-A rating for each, you need to identify and assess risks to these assets. This will involve an analysis of the gap between the current state of the protection and the threats that need mitigating. This stage will identify all the gaps and inadequacies in the current security set up and present it to the information security champions with a cost-benefit analysis so that when security controls are adopted, they are fit for the intended purpose. The accuracy of your risk assessment will be measured by the security incidents that are avoided and realised.

2.3.7. Plan how to reduce risk to an acceptable level

You have identified the risks, now you need to decide how to mitigate their impact (or make the business decision to live with them). Your options for risk management are based on a cost benefit analysis of various options available to handle or accept the risk. Create a risk treatment plan.

2.3.8. Establish pragmatic security policies

Compile a catalogue of policies (AKA policies document, statement of controls, or security manual) that will be the benchmark for decision making. This stage is where you develop the nitty gritty, day-to-day rules that realise the objectives of your high level security policy.

2.3.9. Map out where your security controls should be

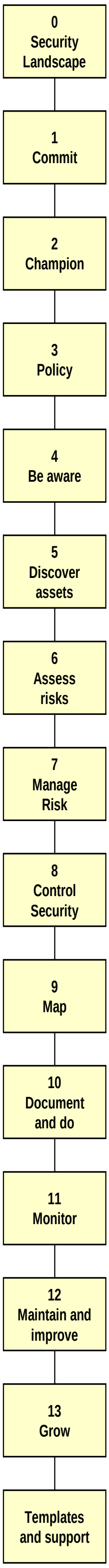
So far, you have taken the risk management approach for identifying and mitigating the risks. Now check your selection of controls against the 135 controls defined by ISO/IEC 27002. As explained, these controls are described in very general terms and no specific interpretation has been provided. The emphasis is on the selection of appropriate controls based on the risk assessment. This will create a statement of applicability which matches the business of your organisation. (When you check that the controls are in place then your statement of applicability will become your first internal audit of your ISMS.)

2.3.10. Write and implement your system security plans, processes, and procedures

Each policy in the statement of controls will be supported by appropriate plans, processes, procedures, instructions and guidelines based on selected practices and, in some instances, products.

Many documented processes will cover several policies or parts of policies. Don't tie your ISMS in knots by trying to maintain a 1:1 relationship between policy and procedure . . . although you must be able to map one on to the other (and it will probably be apparent in your statement of applicability).

The procedures should be detailed and unambiguous enough for every person to follow. These will explain how to assure the security of the business.



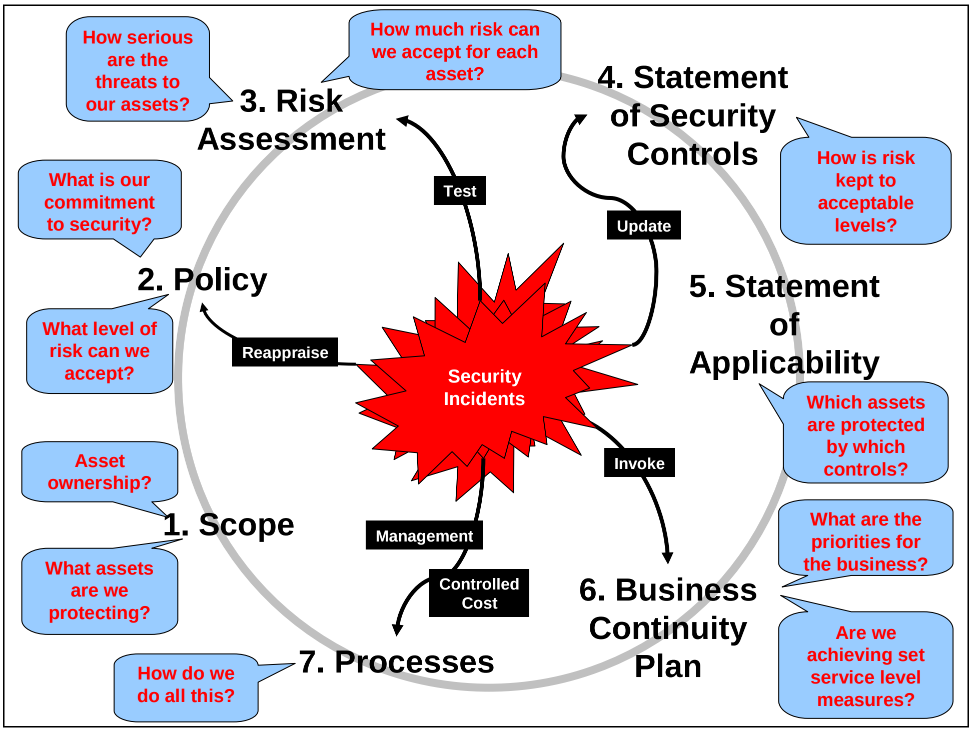

How serious are the threats to our assets?
How much risk can we accept for each asset?
3. Risk Assessment
4. Statement of Security Controls
How is risk kept to acceptable levels?
What is our commitment to security?
Test
Update
2. Policy
5. Statement of Applicability
What level of risk can we accept?
Reappraise
Security Incidents
Which assets are protected by which controls?
Asset ownership?
Invoke
1. Scope
Management
What are the priorities for the business?
What assets are we protecting?
Controlled Cost
6. Business Continuity Plan
Are we achieving set service level measures?
How do we do all this?
7. Processes

Figure 6: A pragmatic and compliant ISMS

There will be 'security incidents'. How you react to these is a test of your risk assessment and planned treatment. Ask whether your level of acceptable risk was contained or exceeded?

2.3.11. Monitor and review the ISMS performance

The effectiveness of how you manage security incidents is a good measure of the effectiveness of your ISMS. What were the outcomes of incidents? If you exceeded the level of acceptable risk to particular assets, have you referred this to the asset owners to consider whether the levels must be reappraised? Is the level of risk increasing or decreasing? Do incidents invoke your business continuity plan[59]?

As if the law is not encouragement enough, compliance with ISO/IEC 27001 requires that you monitor which laws apply to your business and comply with them. Include in your ISMS the processes required by laws and regulations. Your ISMS will provide a framework that will deliver compliance to many of the requirements of the statutes as a by-product of good business management.

The ISMS is not a marketing tool (although it can help); it is an integrated part of your business processes required to assure the information that you handle. Implementing the ISMS is not a one-off job. Good governance demands that it needs to be constantly monitored and reviewed to make sure that it remains faithful to your business objectives.

2.3.12. Maintain the ISMS and ensure continuous improvement

Implementing ISMS will not ensure sudden improvement in the information assurance of your organisation. It provides an opportunity to monitor the security in an organised manner and ensure continuous improvement. Ensure that the continuous improvement actually takes place by defining measures (plan), running your business (do), reviewing those measures for – say - reduced risk, and increase or reduce security activity according to the results of the review (act).

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

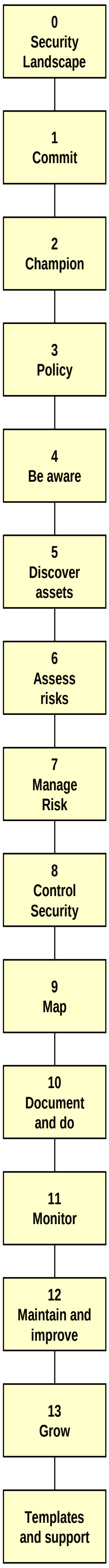
[59] To some the whole ISMS is an extension of the business continuity plan and the process for dealing with incidents is an integral part of that plan. For a more detailed see ISO/IEC 27035 *Information Security Incident Management*

2.3.13. Extending the scope of the security management system

Businesses will change. In fact a complex business may implement an ISMS in phases by concentrating on certain areas or processes and then extending the scope until it is suitably comprehensive. The ISMS must manage change and integrate new scenarios and business activities into current practices or extend those practices as necessary.

The programme of work that follows gives the organisation's management the opportunity to influence the course of the project, ensuring 'buy-in' at all the appropriate stages. It also indicates well-defined milestones against which progress can be assessed.

Each activity is defined with its purpose, its audience, its deliverables and how those deliverables will be communicated in mind. Also, the role of the security expert (who may be the project manager) is shown.



2.4. What does the ISMS comprise?

As discussed previously, information security is built on physical and logical controls implemented by people and technology. This section discusses the elements of the ISMS as you go through each stage of your implementation project, you can tick off the elements that you've put in place. However, one of the greatest threats is complacency[60]. Every aspect will need to be revisited and assessed for suitability for your business and the levels of risk that are acceptable to it as you maintain your ISMS. To achieve this more effectively you will need to focus on two key components Documentation and Management Activities – these are detailed below.

2.4.1. Documentation

Formal documentation of the organisation’s information security requirements lies at the core of the whole process. These documents will mandate the baseline to which existing system security must comply, and the processes that will ensure that such security can be maintained into the future.

In most cases, it will be necessary to separate the various parts of the security policy into one of three types of document:

- **Policies**: These are the top-level documents. They will be mandated by the board, and therefore must be pitched much more at the business aspects of information security, rather than the technical aspects. Policies will contain, amongst other things, references to supporting documents.
- **Standards**: The top layer of supporting documentation, the standards will be the ‘dos and don’ts’ of the security policy. They will set out what must and must not, should and should not be done.
- **Process definitions and procedures**: Documents accompanying the standards which set down how the requirements of the policy will be implemented. These documents will be the most detailed and the most focused.

2.4.1.1. Security policy

The security policy is a published statement that shows management’s intent and commitment for the information security in the organisation. It is based on facts about the critical nature of information held by, and about, your business – this will be identified during risk assessment processes. The security policy statement must strongly reflect the management’s belief that if information is not secure, the business will suffer. The policy should clearly address issues like:

- Why information is strategically important for the organisation?
- What are business and legal requirements for information security for the organisation?

[60] See the table of the top ten IS/IT risks in this Best Practice Guide

- What are the organisations’ contractual obligations towards security of the information pertaining to business processes, information collected from clients, employees etc.?
- What steps the organisation will take to ensure information security?

A clear security policy will provide direction to the information security efforts of the organisation as well as create confidence in the minds of various stakeholders.

Note: Don’t confuse the high-level security policy with the detailed controls used for information assurance, for example whether portable devices are permitted, the complexity of passwords, the use of encryption. These are often also referred to as policies.

2.4.1.2. ISMS scope

The process of carrying out risk assessments and prioritising the protection requirements for individual business areas, based on business impact, should give you a good measure of the critical IT processes that comprise the ISMS. Describing these processes will define the scope for ISMS for the organisation. Your subsequent efforts will be to assure the security of these business activities within the framework of ISO/IEC 27001 applying the appropriate controls to each. An ISO/IEC 27001 certificate will be specific to this scope. If you add more physical locations or business processes that change the scope, you will have to extend the scope of your certificate.

2.4.1.3. ISMS processes and procedures

Just as policies set out what you want to achieve – a secure working environment; a brand with integrity; well-trained and motivated staff etc. etc. – processes and procedures set out how you achieve it. To a degree, the nomenclature is a matter of preference but the de facto standard is to have one or more policies which are implemented by one or more processes. These processes may be enacted by carrying out all or parts of several procedures. To meet the requirements of the procedures you may need to use values derived from one or more standards. This may need some very detailed work instructions to the level of what buttons to press and so on. These documents may also deliver reports to confirm that the actions in the processes and procedures have been successfully completed.

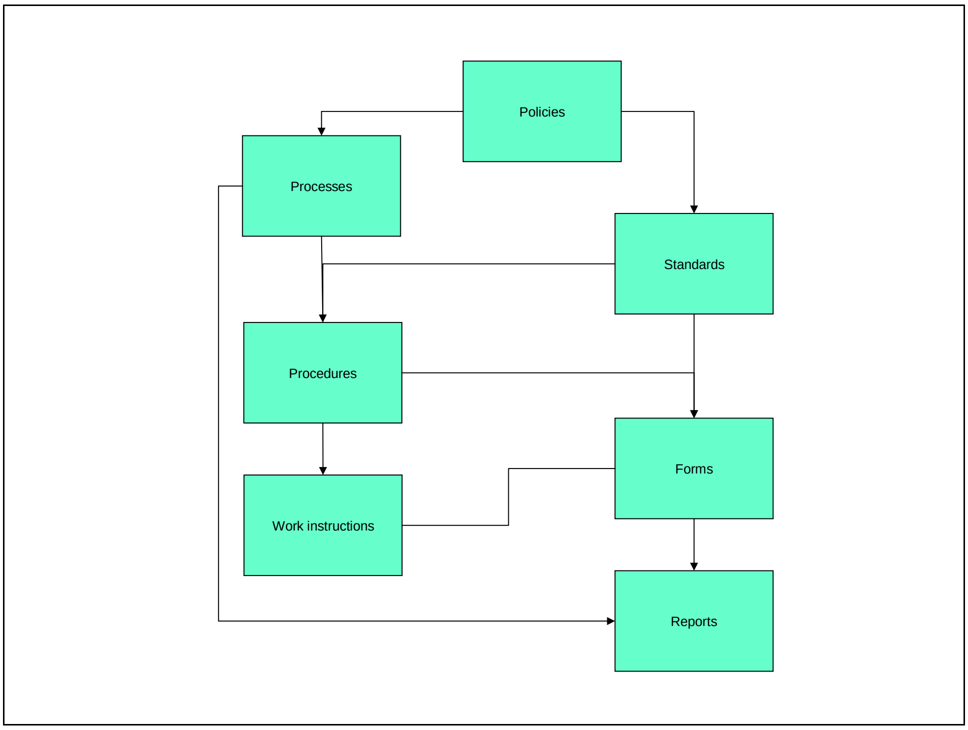
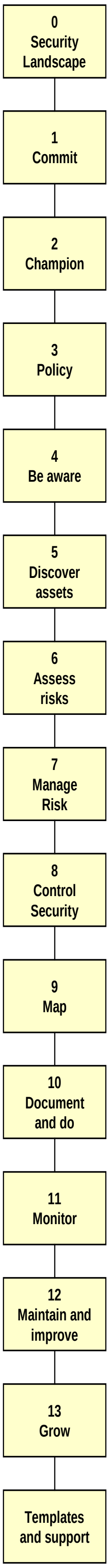


Figure 7: The documentary components of a business management system



2.4.1.4. Risk assessment report

The risk assessment report contains the results of looking at risks to the optimum business environment. This is sometimes categorised in terms of employment, legislation, security, competition and financial risks, and their effects on the confidentiality, integrity, and availability to information assets. It is usual to calculate risks in terms of what information assets are at risk, what could go wrong (the risk), the likelihood of something going wrong and the impact the problem if it does. Reports are usually returned in with levels of acceptable risk expressed in terms of risks being high, medium, or low, or an assigned relative value.

2.4.1.5. Risk treatment plan

A risk treatment plan is the extension of the risk assessment report and covers the tools and methods to be deployed to mitigate the risks and contain them within your acceptable levels. Risks are usually mitigated in terms of what you are going to do about this risk:

- Prevention – stop it happening
- Reduction – reduce the effect if it happens
- Transference – make the treatment some else's problem! (You can’t transfer the risk.)
- Contingency – have ‘plan B’ ready to roll when all goes pear shaped
- Acceptance – recognise that the risk is just too costly to mitigate and so that the organisation shall carry the risk and its impact

2.4.1.6. Operational procedures

These are the ‘how to’s’ that describe the best practices within the organisation. They’ll cover everything from management planning processes to fulfilling orders and the measurement and review processes in between.

2.4.1.7. Records

Records are the evidence of the work being done to assure the confidentiality, integrity and availability of the information. Records will include back-up and firewall logs, incident reports, management reviews, and risk assessments.

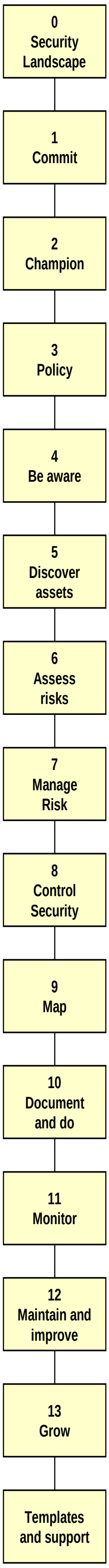
2.4.1.8. Statement of applicability

The success of ISO/IEC 27001 implementation is getting the scope of your management system right – relevant, sufficiently comprehensive, achievable – and the controls that you need to put in place to address the risks within that scope. The statement of applicability defines:

- The controls selected from ISO/IEC 27002
- Where each control is implemented
- If a control is not implemented then a justification of why not

The statement of applicability could be a fairly static document prepared for the sake of internal audits and external assessments. It can be made into a useful knowledge management tool by including:

- The tools and methods used to implement each control.
- Notes and comments about related risk controls.
- Action; by whom; by when to complete implementation, review effectiveness, decommission unrequired equipment etc.



2.4.1.9. Business continuity plan

The business continuity plan is closely linked to your risk assessment and treatment plan that identify the events that can cause interruptions to business processes. Once these threats are identified, the business continuity plan specifies the roles and actions to maintain or restore business operations in the required timescales following the interruption. The plan must be tested and maintained to account for changes to the business. It must reflect the priorities identified in the risk assessment.

2.5. Management activity

2.5.1. Plan-Do-Check-Act

The staple of all good management processes is the simple, repeatable plan-do-check-act cycle that can be applied as an overlay to map all processes. At the highest level this means:

- Plan – What to do? How to do it?
- Do – Do what was planned
- Check – Did it go according to plan?
- Act – How do we do it better next time?

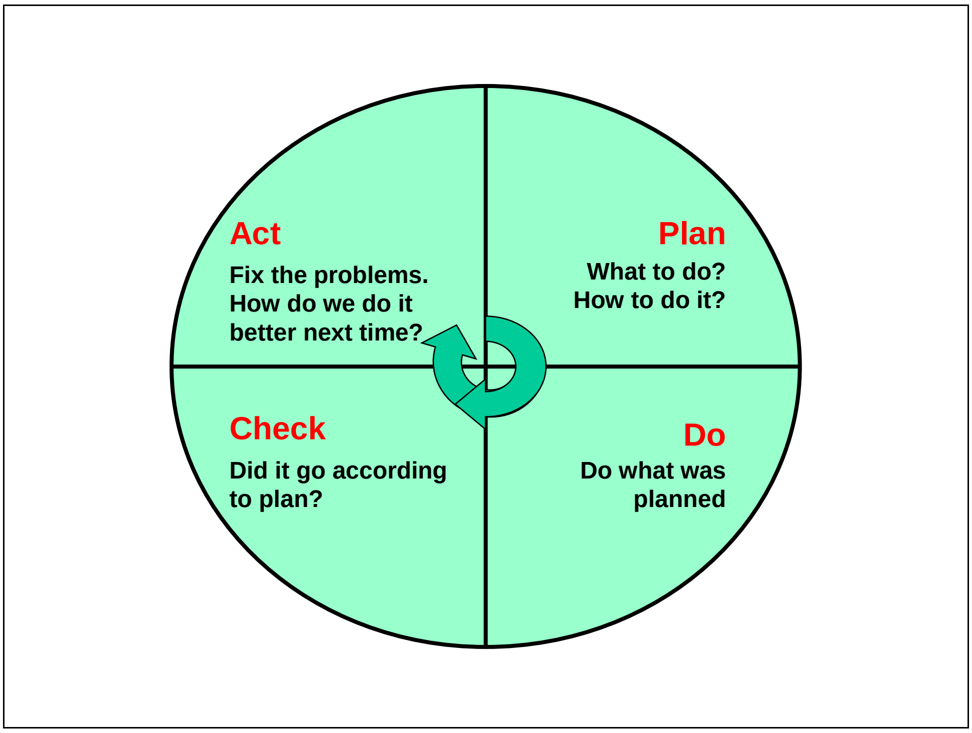

Act
Fix the problems. How do we do it better next time?
Plan
What to do? How to do it?
Check
Did it go according to plan?
Do
Do what was planned

Figure 8: The lifecycle of risk management inferred in ISO/IEC 27002

This method of ISMS implementation follows a plan-do-check-act (PDCA) lifecycle. This is the basic structure of the IT management standards ISO/IEC 20000, ISO/IEC 27001 and (through TickIT[61]) ISO 9001. The quality management standard is so close in practice to the security management standard that organisations that have implemented one will have the basic management system infrastructure to satisfy the other.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[61] *The TickIT Guide: Using ISO 9001:2000 for Software Quality Management System Construction, Certification and Continual Improvement*, British Standards Institution, 2001

2.5.2. Management responsibility

The key to perpetuate the effort put in by the grass roots security practitioners which make all stakeholders aware of security management and give them the wherewithal to comply with security policies, is the demonstration of management commitment. This can manifest itself in chief executive signature on top level missions and policies, the top-down briefings of all staff, and the atmosphere of ‘do as we do’ rather than the too often found ‘do as we say’.

2.5.3. Resource management

Resource management is often an indicator of how much the management is committed to security. Good security management requires equipment commensurate with the assets to be protected, it requires time to learn the techniques and implement the tools. It requires adequate prioritisation with what may seem more obvious first line duties. Good management practice will ‘tool up’ to the job in hand and be prepared to redeploy people and equipment to the most effective positions.

2.5.4. Management review

The management review is a process wherein the ISMS is periodically reviewed for its suitability and effectiveness in implementing the organisation's security policy and objectives. Plan formal review meetings at reasonable intervals. The frequency may need to vary depending on changes in management, significant issues arising from internal or external audit; exceptional security incidents and so on. The agenda for the review would cover (at least):

- Results of internal audits.
- Corrective action/security issues statistics.
- Second/Third Party audit report/findings.
- Policy and objectives review.
- Security policy.
- Scope of certification.
- Risk management.
- Legal and regulatory issues.
- Actions for improvement.

2.5.5. Internal audit

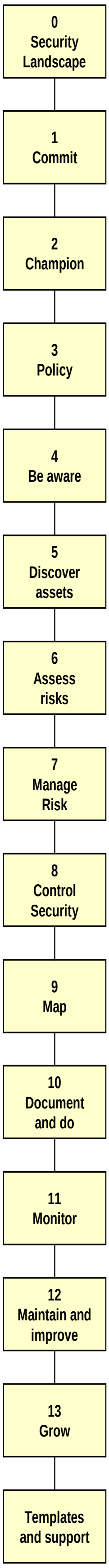
Internal audits are the mainstay of any internal initiative. They give the underlying consistent push to the management launch and give the management information as to what is successful, what is not and what just simply needs reinforcement (in memoranda, briefings, or formal training).

The internal audits need to cover as many of the activities in the management system as possible. Some processes will be audited as part of regular operations. For example:

- On-going password checks.
- Firewall event logging.
- Software license checks.
- Virus tool reports.
- Vulnerability audits.

2.5.6. Continuous improvement

The information that you collect about security incidents and the results of internal audits will be the mainstay of how you gauge your success in continuously improving your management system. You



will need to decide to on the appropriate measures and set achievable, realistic targets within defined timeboxes. Measures may include:

- Numbers of security incidents
- Severity of security incidents
- Time taken to successfully resolve security incidents
- The number of repeated incidents (that is, how effective was the preventive action in eliminating or reducing recurrence)

2.5.7. Corrective action

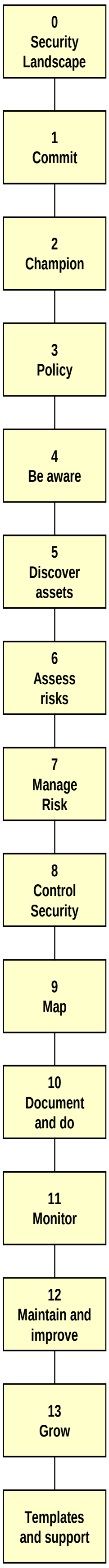
Management systems are not the panacea for all ills but they do provide a calming framework in which to put right what does not go to plan or how to manage 'the unexpected'. Corrective action is the way of dealing with the problems that will arise. The aim of corrective action is to:

- Solve the problem
- Solve it effectively
- Only make new mistakes

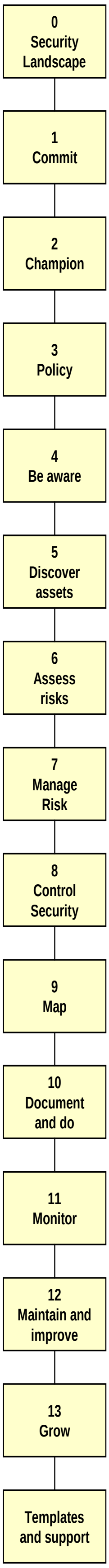
2.5.8. Preventive action

Preventive action takes the longer view. Preventive action takes the knowledge and resources available to prevent security incidents from happening. These may include procedures, or new or strengthened logical and physical controls.

Now let us look at each stage of the project in detail . . .



3. Implementing or improving an ISMS: the stages in detail



Each of the thirteen stages of implementing, improving, or extending an information security management system is described in a standard (sic!) format of six components:

(1) Purpose of each stage of the project.
The objectives of that stage, so that you are clear about the reasons for doing it.

(2) Where does it get you with ISO/IEC 27001?[62]
Which of the 135 controls should be selected from ISO/IEC 27002 and implemented during the respective stage?

(3) The 'audience' for each stage of the project?
You should not be alone in the realisation of information security so this subsection sets out the stakeholders who need to work with you.

(4) Which deliverables come in each stage of the project?
Some stages see the creation of certain tools, documents, or building teams.

(5) Techniques for successful completion of each stage of the project.
Best practice should be shared and here we share the methods for successfully creating and implementing an information security management system.

(6) The role of the security expert during each stage of the project.
Sometimes you'll have the relevant skills; sometimes you may need that extra help. Here we describe how to get the best value from any external consultant that you may retain.

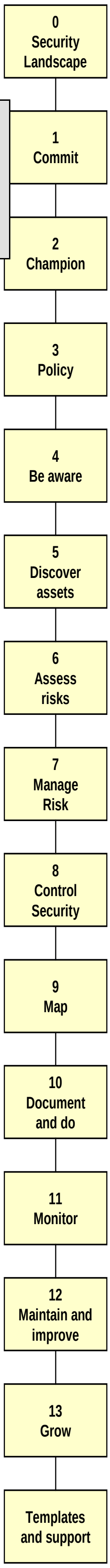
3.1.1. Who is a security expert?

One of the key issues here, is understanding what you can do yourself and when you need specialist help. This may be less apparent in information security because we can all follow 'common sense' – don't leave sensitive business papers on display or a laptop computer on the back seat of the car. Where issues become more blurred is the 'ease of use' that information technology places at our fingertips. Even if you know what a 'firewall' is and you can install it, do you know what the optimum security configuration for your circumstances are? Even the phrase 'optimum security configuration' should have you treading with care . . . the honest question is, do you know not only how to set it up, but how to test it too? The answer is likely to be no unless you are a security specialist. You will need assistance.

The smaller your organisation, you are less likely to have all the skills you need 'in-house' and so your will be more likely to engage a security expert to facilitate the implementation of the ISMS across the business. Larger organisations may find this useful to keep a fresh view on a recurring concern. Mature organisations who have their ISMSs certificated should find that a good assessor can fulfil this role (but not during the development of the ISMS). To help, we have highlighted the role of the security expert at each stage so that you can plan how much help you need. Remember to consider the level of trust that you must have in such an expert.

[62] This best practice guide is all about getting the right level of control in the right place. Therefore it focuses on using the catalogue of controls in ISO/IEC 27002. However, to select and implement these controls you require the process oriented part of the security management process which is covered by ISO/IEC 27001. As a consequence of this, not all sections will have a subsection 'Where does it get you with ISO/IEC 27001 compliance?'.

4. Stage 1 - Persuade Top Management of the Need to Act on Security Issues



4.1. Purpose

No matter where an idea comes from – staff, customers or the company board – it must carry the approval of top management to ensure that it receives the resources needed and remains at the right level in the priorities list. This stage collects any issues identified to date, presents the business case for the implementation of the ISMS and hand the baton to those who will see it through the forthcoming stages defined in this chapter.

4.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

- 6.1.1 Management commitment to information security

4.3. Audience

It is ideal to include the organisation's executive and non-executive management. At the very least the ISMS development project must have the backing of the Chief Executive Officer and have a budget for staff time and equipment that will mean that local managers will not feel that their targets are threatened.

4.4. Deliverables

A statement of commitment to protect the information assets of the organisation, endorsed by the chief executive officer on behalf of top management such as the board of directors.

4.5. Successful techniques

Use a high-level risk assessment to show how actions are required to mitigate threats to the business.

Get the authorisation from top management to set up a security coordination activity. Carry this commitment through the management and leadership of the organisation.

Kick-off a campaign of security awareness, education, continuing education, and motivation of staff. This is described in more detail in 'Compose and agree your high level security policy' below.

4.6. The role of the security expert

It is often difficult to promote change from within and reasons may vary from tensions between departments to being unable to allocate time to both justifying the need for an ISMS and getting on and implementing one. Here your external expert can provide the wider view, give the benefit of experiences that you will not yet have had time to accumulate. In extreme cases the expert may be able to make more forceful points, because he or she will not have to face your colleagues or management the next morning!

5. Stage 2 - Appoint Security Champions to Represent all Activities

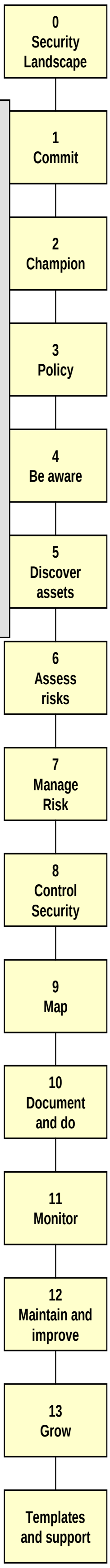
5.1. Purpose

After you have issued the security policy statement, establish structure for managing security within your organisation. This is necessary to ensure the organisation’s involvement in identifying and implementing various security measures.

The implementation of the ISMS will need the buy-in from the whole organisation, not just initially, but also when threats are identified or incidents occur. You will need a mechanism whereby you can collect a holistic view of the impact of security issues and a channel for disseminating the information and actions. You need a team of information security champions that represents the makeup of the organisation and who will coordinate the implementation and maintenance of the controls that are selected.

You may decide to implement or expand your ISMS in phases. This has the challenge of secured parts of the organisations having to interact with other that may be unsecured. Manage these relationships with service level agreements (SLAs)[63].

Deperimeterisation has its effect here. An organisation needs to concern itself not only with its users, but also its supply chain, those its thrall, and the social and regulatory regime within which it operates. Make sure that representation is wide enough to manage all the interfaces with your ‘extended’ business.



5.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

- 6 Organizing information security
- 6.1 Internal organization
  - 6.1.2 Information security co-ordination
  - 6.1.3 Allocation of information security responsibilities
  - 6.1.4 Approval process for information processing facilities
  - 6.1.5 Confidentiality agreements
  - 6.1.6 Contact with authorities
  - 6.1.7 Contact with special interest groups
  - 6.1.8 Independent review of information security
- 6.2 External parties
  - 6.2.1 Identification of risks related to external parties
  - 6.2.2 Addressing security when dealing with customers
  - 6.2.3 Addressing security in third party agreements

5.3. Audience

Draw representation from across the organisation covering sites, divisions, departments, and functions.

[63] The catch-all contents of an SLA are contained in an appendix.

The security organisation should consist of the following, depending on the size of your organisation. In a small organisation, once the ISMS is established, this could be a part-time role for one person. The objective should be representation and understanding of the business processes:

- An Information Security Officer for overseeing the day-to-day implementation and maintenance of the ISMS.
- An information security steering panel or committee of departmental champions[64]. Include:
  - Representatives from key business and technology departments
  - Those responsible for managing third-party relationships such as landlords and outsourced services
  - Those responsible for contact with authorities such as the emergency services
  - At least one executive board member
- Again, depending on the size of the organisation, the panel may include representation from other security teams for example:
  - Incident response team
  - Security maintenance team
  - Security training team
  - Disaster recovery team
  - Security policy and process owners

The members of these teams could be either full time members or part time, depending on the size and requirements of the organisation. In smaller organisations, all these activities may be part of the day-to-day responsibilities of the ICT infrastructure team.

5.4. Deliverables

A coordinator for information security or a representative panel with a process-based constitution:

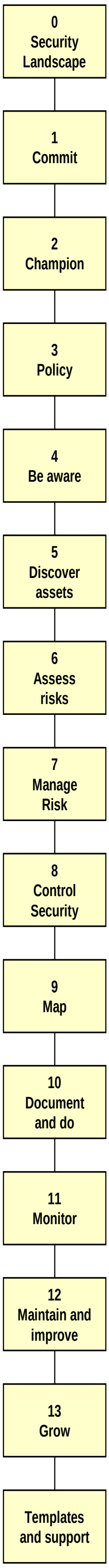
- How it is comprised
- When it meets or how it is called together
- The authority it has and the escalation process if that authority is exceeded or undermined

5.5. Successful techniques

Contact the managers and team leaders, explain the purpose of the security coordination activity and call for nominees to take part. You will need to assure the participants of the authority to convene the security coordination activity and estimate the likely commitment that will be required[65].

The Information Security Officer:

- Coordinates the activities of all the security-related teams
- Defines the security roles and responsibilities for identification and protection of various information assets by specific individuals, including end-users, who are responsible for handling these assets
- Designs and implements (or delegates and coordinates) detailed security policies to cover all the areas to be addressed by ISMS



[64] Consider the impact of having this headed by the Chief Executive.

[65] Remember that first stage of management buy-in.

- Coordinate periodic reviews of the security efforts by internal and external experts as well as auditors
- Has frequent contact with managers and team leaders

Use service level agreements to manage the relationships between departments where the security status of one is not commensurate with that of the other. Use the lessons learnt in the implementation of these SLAs to create permanent working practices in your ISMS. You may find it useful to create information assurance plans that focus on the mitigation of risk to particular systems. You will derive lessons from the system-based practices in such plans. The practices therein will become standard across the organisation and form the foundations of your developing ISMS.

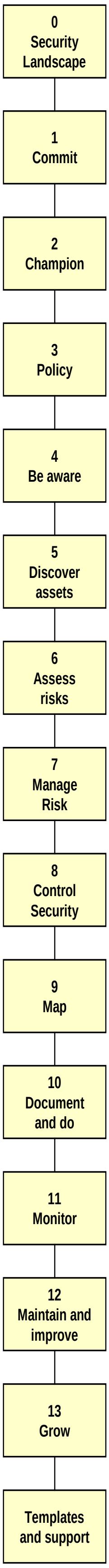
5.5.1. Typical things to think about . . .

As we have tried to make it clear throughout this best practice guide, standards implementation is a practical activity that is governed partly by risk and partly by the size of the organisation that is investing in its future. Therefore, smaller organisations may innovate around the water cooler, capturing the wisdom later, whilst larger organisations may need more formal mechanisms to ensure that a keen observation isn’t lost to the corporate body like tears in the rain.

The champions of security issues across the extended organisation are strategically placed to gather, maintain, and protect the interests of the organisation by watching over the individual parts. They get involved in setting policy, ensuring co-operation and establish a transient virtual organisation, within the organisation, whose interest is information assurance. They can solve problems with everything from an informal chat or the establishment of service level agreements (SLAs)[66] to manage the boundaries with areas not yet coming under the scope of the ISMS. Security champions need to keep abreast of the risks to their specialist areas and so will benefit from keeping up to date with relevant institutes[67] and other special interest groups.

5.6. The role of the security expert

Roles and responsibilities can be difficult to allocate effectively and there is often a tendency in establishing an ISMS to create more roles than necessary. Work with your security expert to settle on the right breakdown of rolls for your size of organisation and the activities it engages in. Your knowledge of your organisation and the experts clinical view of ISMS theory can deliver an ISMS based on roles that take account of what staff already have to do. This means that you may be able to create an ISMS without having to allocate too many new responsibilities.



[66] Remember ISO/IEC 20000 for *IT Service Level Management*

[67] Not least the upcoming Institute of Information Security Professionals

6. Stage 3 - Compose and Agree Your High Level Security Policy

6.1. Purpose

This is where the information security champions works with top management to set the scope of the management system and high-level security policy. Policy documents form the core of any ISMS. They formally set down the requirements of the system, and provide the mandate from the top of the organisation that ensures the ISMS can be enforced operationally. All questions of security lead back to this policy and it must be regularly reviewed by top management for its effective implementation and continuing relevance to the business that the ISMS sets out to protect.

6.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address:

- 5 Security policy
- 5.1 Information security policy
  - 5.1.1 Information security policy document
  - 5.1.2 Review of the information security policy

6.3. Audience

The scope and policy should be drafted by those who coordinate the information security activities, led by the Information Security Officer, and endorsed by top management.

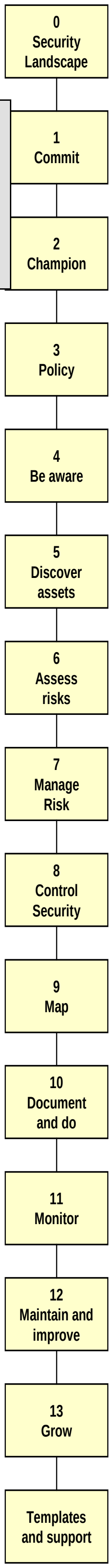
6.4. Deliverables

A high-level security policy which must be:

- **Detailed and specific**. Make it relevant to the mission of the organisation rather than just a generic rallying call copied from a website of templates.
- **Practicable**: it does not make demands that cannot be resourced.
- **Auditable**: to stay fresh, you must be able to verify the implementation of a policy so that you can adjust your working practices to fit it and keep it relevant to your business objectives.
- **Bounded** so that other divisions, subsidiaries, and other organisations in the supply chain know where they stand. Make it clear which information systems, networks, and information assets, business activities and locations are involved.
- **Measurable**: You may not want to include detailed metrics in your policy statement but at least include a specific reference to what measures show the effectiveness of your ISMS
- **Certifiable**: whether you want a certificate on the wall or not, have management processes which deliver enough tangible evidence of having been carried out to show compliance with the relevant standards.

6.5. Successful techniques

Think about how information security is important to the organisation so that you can prepare a scope that doesn't include anything unnecessary and so weaken its message or credibility. Align the security policy with the organisation's mission statement - it may form part of it. Display the policy prominently as a reminder for staff and as an encouraging sign for visitors.



Sample policy

The Organisation is unreservedly committed to satisfying its customers through:

- The delivery of customer-centric information services, networking, accreditation, personal development, research, software and other managed information technology services.
- Harnessing the knowledge, experience and enthusiasm of staff to improve quality and add value to our products and services.
- Maintaining the security and integrity of the intellectual assets of the Organisation for its customers.
- The continuous improvement of our working practices, and the products and services delivered.
- A network of partners who are able to deliver complementary, and exemplary, products and services.

In support of this policy, the Organisation operates a management system of standards and procedures within which we manage and control all our project, product and service activities.

The management system is based on the requirements of the pertinent parts of ISO 9001, TickIT, and ISO/IEC 27001, the National and International regulatory framework, and is independently assessed for compliance.

The successful implementation of this policy is measured by:

- Feedback from customers through formal surveys and ad hoc contact
- Analysis of products and services by post-project/service delivery reviews and event feedback
- Regular top management review of key performance indicators including:
  - The cost and frequency of security incidents
  - The achievement of business continuity objectives
  - The containment of risk to information assets within predefined, acceptable levels
- A risk-based programme of audits of staff and systems to ensure competence and capacity are maintained

The implementation of this policy is mandatory and is to be observed by all those who contribute to the Organisation’s products and services.

Figure 9: Model security policy

And be clear what this policy applies to:

The information security management certification applies to the provision and operation of a secure environment for:

- Customer services
- Research and development
- Project management
- Advisory services
- Internet services, and Internet solutions
- Internal communications

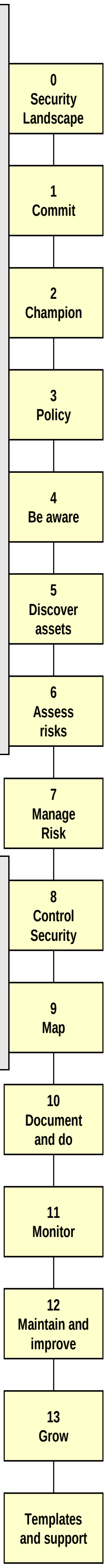
Figure 10: Sample scope of an ISMS

6.5.1. Typical things to think about . . .

Think about the use and distribution of what will always be a knot-in-the-handkerchief of sanity whenever a new avenue of opportunity opens. It’s the chance for you to dispel the myths that security is all cloak and dagger stuff and that it’s about the practical day-to-day protection of your intellectual property. Make it the springboard to all those people, processes, and technology that are the realisation of your ISMS.

6.6. The role of the security expert

Use your security expert for draft or assess your draft of a security policy that can be aligned with the activities of your business and the company spirit of your staff. Getting this right is so important because it is the anchor for the whole ISMS – and may even be more stable than the scope of the ISMS. You must get the buy-in of the top management for the policy and the independent view of the security expert can help you keep it independent of the personalities and agendas that may affect its emphasis.



7. Stage 4 - Create Security Awareness: Train and Educate Staff

7.1. Purpose

Information security will involve every member of the organisation be they responsible for designing products, delivering services, or maintaining the areas in which the designers work. Information security touches the whole organisation whether they are ICT users or not. Each person has capability of sabotaging the information security through ignorance, or with malicious intent. A careless comment about a customer may do expensive or irredeemable damage to the organisation's brand.

Education and training is needed to explain each individual’s role in maintaining the information security and his/her responsibilities towards every information asset that they handle or have access to. Education and training should be comprehensive and adequate to ensure that each person clearly understands the security policies of the organisation, various security risks and threats, the processes and procedures to be followed, and finally consequences of not abiding by the security procedures.

7.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

- 8.2 During employment
- 8.2.2 Information security awareness, education and training

7.3. Audience

Education and training programmes need to be tailored to fit the responsibilities and attention spans of:

- Top management
- IT staff
- End users
- Site services and maintenance staff
- Contractors

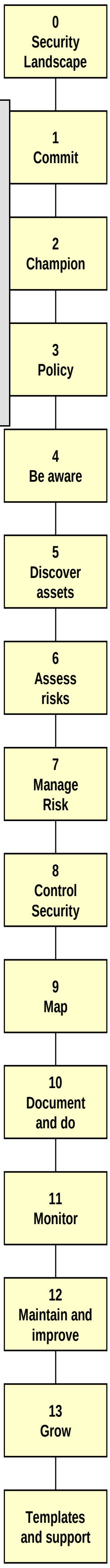
The content of the training programmes should fit with the relevant importance of the information assets of the organisation as determined by the risk assessments. Remember to consider making staff aware as they join, move through, and leave your organisation.

7.4. Successful techniques

You note that some of the recommendations below refer to artefacts from the ISMS that will not yet exist if you are creating a new system. This is because awareness is not a one-off display of encouragement but a rolling programme that must take account of staff turnover and changes to roles where staff may take on responsibility for increasing sensitive information. Make sure that the relevant contracts are kept up to date for full and part time staff, including partners and contractors. Carry these requirements through to disciplinary procedures, and sanctions so that staff and suppliers are equally aware of the importance of managing information assurance within different relationships.

Prepare an annual schedule for the training and awareness programmes to ensure that all the current staff are trained and that new staff are fully aware of their responsibilities. You will probably need to give new staff some rudimentary training immediately. Be ready to train staff whose responsibilities change, especially when they move to a more secure area of working.

Be as creative as necessary. Consider the use of:



- Formal presentations
- Question and answer sessions
- e-learning
- Slogans on posters, intranet and newsletters
- Special security bulletins and newsletters – in print or e-mail
- Competitions and suggestion boxes

When security incidents occur, make sure that staff are aware of anything that has lessons to be learnt – or to show how the ISMS was effective – so that the theoretical incidents suggested by the risk assessments are shown to really happen and require constant scrutiny.

Security awareness is rather like creating a human firewall and indeed the Information Systems Security Association run a website with just that name[68].

A survey from the original National Computing Centre in the application of security policies[69] showed that training is proven to be key. Simply, promote awareness and you get awareness. An informal or formal campaign has a significant positive effect on end-user awareness and this is seen in organisations with an on-going security awareness programme and/or regular security briefings for end-users.

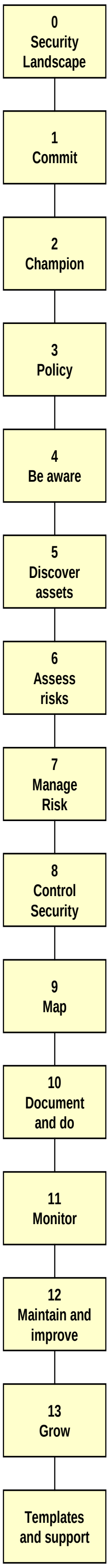
You need to make it clear that all staff have a responsibility for protecting the information assets of the organisation. It is the individuals' role in maintaining security that can make a difference. Educate staff to 'think secure' so that they realise their responsibilities towards every information asset that they handle/have access to. The real security risks and threats are the consequences of not abiding by the security procedures.

Discuss the consequences of poor security with them. You will need to consider the personalities involved. You may need a few scare stories from reliable sources, such as the biannual Security Breaches Survey published by DTI, but balance this with lots and lots of positive steps. Cover as many of the issues that may be faced as possible and discuss the policies and standards that are put in place to deal with them. Make sure that some of your messages are conveyed through leadership. The NCC survey referred to above showed that where awareness is high amongst end-user managers, policy and procedures are enforced.

Explain simple practical issues such as where do they find the complete policies and standards for your organisation? What are the characteristics of a security problem? Where do they report a potential incident? Go into more details and explain the security policy and some of the basic controls that are in place to mitigate risk. Explain some 'Whys' but there is no need to for your users to understand the algorithms of PKIs, VPNs etc. but they should know when to use them.

Explain the process of certification to all so that they can understand what will be expected of them if you want third-party endorsement. If you involve your assessors early enough – and you should – it is an opportunity to embed the assessment into your management process and ensure that the whole organisation shares the triumph when a certificate is awarded.

And don't forget to have a reminder campaign to keep staff mindful of security. Also being true to our plan-do-check-act model, you must evaluate effectiveness of the education and awareness programme. Consider metrics such a rise in reporting or a rise/fall in incidents. Look at the nature of the incidents. Do security incidents suggest need for more training? Do there seem to be far fewer reported incidents than expected? React according to increase awareness activities or target them on specific groups or issues.

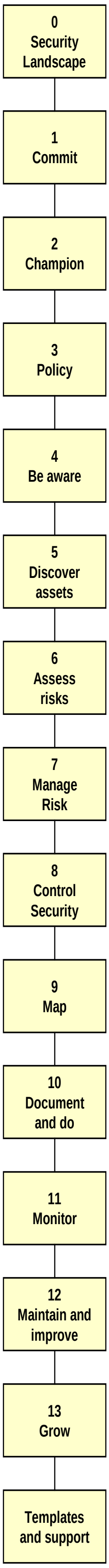


[68] www.humanfirewall.org

[69] NCC, Survey of Information Security - Policy and Practice 2004

7.5. The role of the security expert

Give your independent security expert the platform at staff briefings to show that there is a connection between the objectives of the ISMS and the wider demands of the markets where your organisation operates. This will reinforce the external benefits of the ISMS rather than running a risk that it may be seen as ‘just another management initiative’.



8. Stage 5 - Identify and Classify the Assets

8.1. Purpose

It is difficult to protect what you do not know that you have. The purpose of this phase is to identify the organisation's information assets - which may vary from computers, databases, or printed and hand-written documents - and know something about these assets. This is also where you broaden the championship of security and make sure that each asset can be attributed to an owner. Once you know something about what you have, the information security champions can work with the asset owners to determine the levels of acceptable risk and make sensible decisions about the level of protection required to keep public information accessible and private information available to those who need to know.

8.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

- 7 Asset management
- 7.1 Responsibility for assets
  - 7.1.1 Inventory of assets
  - 7.1.2 Ownership of assets
  - 7.1.3 Acceptable use of assets
- 7.2 Information classification
  - 7.2.1 Classification guidelines
  - 7.2.2 Information labelling and handling

8.3. Audience

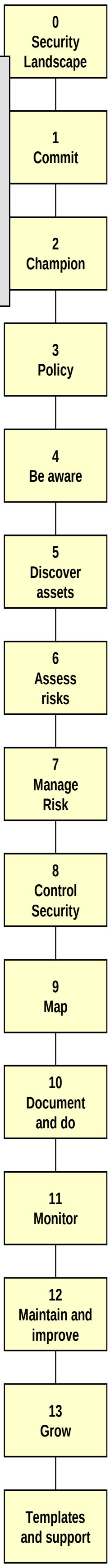
The information security coordinator (or a perhaps the information security champions in larger organisations) will need to commission an internal audit of the organisation's assets. If you have a formal management system in place, you may be able to appoint internal auditors to this task. The breadth of the investigation may be an opportunity to involve more staff in the initial work of the ISMS and get their buy-in to the control measures for protecting those assets they work with.

8.4. Successful techniques

The key word here is **asset**. Make your risk management, 'asset-based'. Rather than think generally about the risks first think about what it is you are trying to protect. Consider your business' assets - you could extend this to everything down to the paper clips but let's restrict ourselves here to your information assets. This is where ICT risk management is often misplaced; it is relatively easy to replace hardware but the information stored thereon may have taken years to design or accumulate.

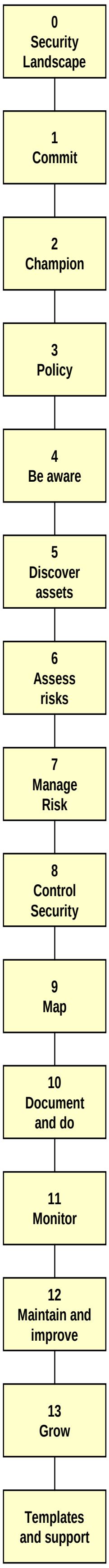
In your first – and possibly some parts of future catalogues – be prepared to group assets together. For example, financial records, seminar presentations, or CRMS database. This may help to keep up the discovery of assets rather than drilling down too soon. This may result in you becoming obsessed with completeness in one area at the expense of initially useful generalisation. The wider view catalogues much more and maintains buy-in from areas which may feel that if they’ve not been involved early on, the ISMS may not apply to them.

Since there is no ‘correct answer’ for information security, as discussed in the previous chapter, it follows that all policies, standards, and procedures must be created to exist in the context of the organisation’s own systems and processes.



To help achieve this, it will be necessary to create a detailed, complete and accurate inventory of existing information systems. This phase of work can be simple and straightforward – especially in small organisations – or virtually impossible, if there are data-centres full of badly-documented and occasionally legacy kit to be evaluated.

This exercise is also an essential component of the creation of the detailed asset register required by the ‘Asset Management’ section of the standard. Fortunately there are various methods by which these daunting projects can be broken down into more manageable chunks. There are also tools available to at least partially automate the discovery phase.



8.4.1. Typical things to think about . . .

8.4.1.1. Asset identification

Use an identification scheme that uniquely identifies each of the assets listed above, preferably as part of an organisation-wide asset tracking system. The purpose of this is to avoid duplication of the effort. For all the assets, record:

- A list of the assets and their owners
- The replacement value of these assets[70]
- Location of the assets
- The acceptable use to which assets may be put
- Level(s) of acceptable risk to each asset[71]

You are likely to end up with two types of asset in your register:

Information Assets - Physical (off the shelf)	**Information Assets - Logical (created)**
· Fax machines/printers	· Project data/products
· PCs and laptops	· Databases
· PDAs	· Training material
· Routers	· E-mail
· Servers	· Personnel records
· Software products (e.g. COTS): – Software tools (Office Infrastructure) – Software tools (development and support)	· Financial records such as: – Business plans – Tax records
· Tablets	· Software source code and web pages
· Telephones (fixed and mobile)	· Research papers

[70] Everyone should aspire to having an accurate valuation of their assets but as we shall see, this should not delay the process of ISMS development and improvement. A relative valuation can be effective and we suggest how to this effectively below.

[71] You may find it easier to deal with this in the next stage.

Information Assets - Physical (off the shelf)	Information Assets - Logical (created)
	· Customer licenses, contracts and agreements with suppliers/third parties
	· Quality/Security Management System documents
	· The asset register itself!

Table 3: Examples of the information assets you might expect in a register

8.4.2. Information access classification

All information must be clearly classified for confidentiality, integrity and availability. For example: statements of copyright and limitations on liability must be clearly positioned. Access to information is determined by the classification awarded to it by your policies. The classification tells you how information should be handled.

Classification	Permitted recipients
Unclassified	Considered publicly accessible. There are no requirements for access control or confidentiality.
For internal use only	May only be seen by members of staff or contract staff and partners who have signed an approved non-disclosure agreement.
Commercial in confidence	May be distributed to targeted recipients of (say) proposals.
Restricted	May only be seen by Executive Directors and nominated members of staff.
For addressee only	As it says.

There may be information assets that take advantage of technology to give different levels of access to different staff. For example a database of staff information may be used to extract an internal telephone directory and record personal information about each member of staff. The directory information would be available to all but the personal information would be available to designated Human Resources staff only.

8.4.3. Finding assets around the network perimeter

When studying the perimeter of a network, it helps to be able to categorise the various network segments by trust. A simple but effective approach is to define networks as trusted, semi-trusted and untrusted. Trusted networks are those that the organisation controls completely (especially all points of the perimeter), and which are accessible only to trusted and vetted individuals. Semi-trusted networks are those controlled by the organisation, but accessible by third parties (such as DMZs and extranets). Finally, untrusted networks are those that are totally outside the control of the organisation – for example, the Internet, or a partner organisation's network. This terminology will be used throughout this section.

Conceptually, the perimeter of a network is like the fence around the edge, with patrolled gateways cut into it. In terms of system analysis, however, the perimeter is defined as being all devices that separate the trusted network from another network – examples being firewalls, routers and even remote access servers. In a small organisation the trusted network perimeter may comprise one solitary firewall. In a large organisation with a multi-site WAN, it will be made up of many firewalls, many modems, perhaps some broadband or ISDN connections, and often routers connected to third-party networks as

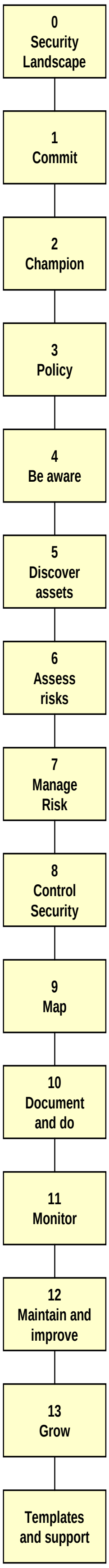
0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

well. Perimeter points may even include CAT5 network sockets that are in a public or insecure area, or inadequately secured wireless access points.

For the network inside a perimeter to be considered as genuinely trusted, then the organisation must have full control and visibility of all of the devices that form the network perimeter. This has particular implications in environments that are at least partially outsourced.

The establishment of the perimeter will require the discovery of the following assets:

- Network connectivity: Leased lines, broadband connections or ISDN – nearly every organisation has at least one of these forming the infrastructure of their connection to the Internet. Many will have several, providing backup connectivity, or links to partner organisations. All such connections must be included on the register.
- Gateway devices: The above lines will terminate on routers or similar gateway devices (for example, ADSL modems). Regardless of whether the gateway device is managed by the organisation itself, or by its bandwidth provider, it must be included on the register.
- Firewalls: The real strength of the perimeter lies in the devices specifically responsible for mediating traffic between the untrusted and trusted segments of the network. In most cases, these will be firewalls, and will be the next hop after the gateway device. These must be included on the register.
- VPNs: Although these are not usually devices in their own right, they offer a form of virtual connectivity between the organisation’s trusted network and another network, and hence need to be considered as a component of the network perimeter. This applies to both network-to-network VPNs (such as those implemented to the IPSEC standard) and client-to-server VPNs used for individual dial-up and access via the Internet, and usually implemented with PPTP.
- Routers and modems: These can be the most difficult of perimeter devices to locate, because they are small, cheap, and – especially in larger organisations – easy to introduce as a pragmatic method of circumventing the security restrictions of a firewall. For modems, some information can be gleaned from telephone installation records (in many cases, the modem can be identified by the presence of a separate, analogue line). Physical auditing can often locate modems, but this is becoming increasingly difficult as internal modems replace the distinctive boxes with flashing lights. If the organisation has an established range of telephone numbers then they can be called in sequence to see if any are answered by a modem. Some security consultancies provide this service (known as war dialling). ISDN modems must be considered in this context as well. All modems must be placed on the register of perimeter devices.



The register of perimeter devices must include certain critical information that will be used in making decisions during the development of the security policy and its supporting documents. The purpose of all devices must be identified, along with the owner of the device.

8.4.4. Catalogues and classifications

Catalogue the critical business processes and the systems (human and ICT-based) which support them. Each process or system will involve work on or the delivery of one or more information assets (not necessarily visible to the customer). These information assets utilise other critical components like key staff knowledge or training, software, hardware, physical and infrastructure facilities to perform designated tasks efficiently securely. Without maintaining this catalogue you will not be able to identify all the assets which need protection. Once you have this catalogue or inventory, devise a scheme for classifying the assets, based on their criticality towards **c**onfidentiality, **i**ntegrity and **a**vailability of information:

- Confidentiality –the most confidential information is for certain customers and/or staff only; the least confidential information is available to the public.

- Integrity – is at its highest when information must be 100% numerically accurate or entirely unambiguous. Integrity is only a minor concern if it will tolerate a wide margin of error.
- Availability – the highest level of availability is information that must be available immediately. Other information may be safely managed without for hours, days or weeks depending on your risk assessment.

Depending on the size of your business, it may be worthwhile to list the 'owner' of each information asset to make sure that you keep up the buy-in of your team. This will be key to identifying the real risks and what to do about them.

Now let's try getting a bit scientific. For each asset, list each risk, its relative value, the probability of this risk happening, and the severity or impact of the effects. Use your good judgement - and that's worth a lot - to score a relative value, probability and impact. One simple, but effective way of scoring is to use values ranging from 1 to 5 (1=low, 5=high). Now you can 'calculate' your business' exposure if you multiply importance, probability and severity together, to derive a joint value.

These numerical values may represent a scale such as:

Attribute	Relative score	Effect/business impact
Confidentiality	5	Usually for certain customers and/or staff only
	1	For public information
Integrity	5	Must be complete, 100% numerically accurate or unambiguous
	1	Will tolerate a wide margin of error or some missing components
Availability	5	Must be available immediately
	1	Should be available within 1 week

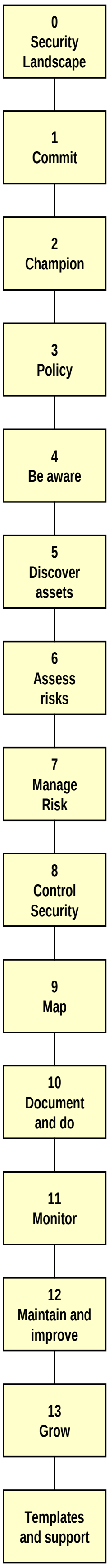
This valuation is a pragmatic way of starting a risk assessment process (see the next stage) that can be consistent and repeatable. You create a catalogue of what you need to secure. Here’s a small sample

Asset	Owner	Ranking for			Totalled Rank (C+I+A)	Importance on the scale of 1-5
		Confidentiality	Integrity	Availability		
Database	Org.'s DBA	5	5	1	11	4
Street Hardware	Local Authority	1	4	2	7	2
Operator Logs	DIAMOND Sys. Admin	4	5	1	10	3

Where the importance on the 1 – 5 scale is the rounded average of the Totalled Rank (R=C+I+A) to retain a relative importance on the scale of 1-5.

8.5. The role of the security expert

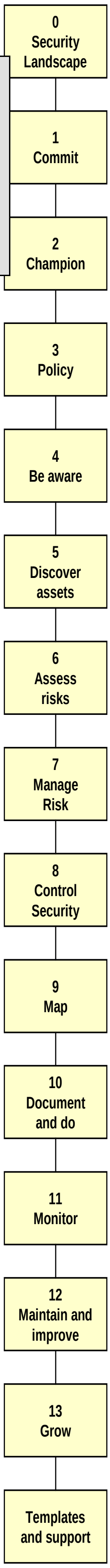
Cataloguing your assets is fraught with the usual problem of list making – how can you be reasonably sure of including all that you need to. The security expert can, by questioning you or your colleagues, help to divine the existence of many day-to-day items that may be overlooked.



9. Stage 6 - Assess the Risks to Your Information Assets

9.1. Purpose

Once you have a comprehensive list of all the critical assets whose failure could impact on the business and the C-I-A rating for each, you need to identify and assess risks to these assets. This will involve an analysis of the gap between the current state of the protection and the threats that need mitigating. This stage will identify all the gaps and inadequacies in the current security set up and present it to the information security champions with a cost-benefit analysis so that when security controls are adopted, they are fit for the intended purpose. The accuracy of your risk assessment will be measured by the security incidents that are avoided and realised.



9.1.1. Security must make sense: relevance through risk assessment

It is very easy, in the quest for total security, to lose sight of the purpose of the whole exercise. If the security measures that are being put in place cost more to implement and/or run than the amount that the business could conceivably lose if such measures were not present, then something has gone wrong.

This applies particularly to organisations that are planning to acquire accreditation to ISO/IEC 27001. The process of acquiring such accreditation can involve enormous, extraordinary quantities of work. One sizeable organisation found itself employing a team of ten consultants for a year and a half, who between them generated so many documents that they were also obliged to employ two full-time librarians. The organisation in question was not unjustified in this – they had a pressing business requirement to thoroughly implement the entire standard. But, as has already been pointed out, not every organisation needs to carry out a total implementation, nor is there any obligation to do so. In the vast majority of cases, it is necessary to decide which parts of the standard to implement against particular information systems, and to be prepared to justify the omissions. This scalability is one of the characteristics of ISO/IEC 27001 that makes it viable for smaller organisations.

The process of making informed decisions about which parts of the standard to implement across the entire organisation and upon individual information systems is key to exploiting the benefits of scalability. It hinges on a series of risk analyses and business impact analyses that must be performed, so that the variables involved in these decisions may be quantified.

- Identify and assess risks to assets
- Gap analysis between the current state of the protection and the threats that need mitigating
- Present it to the information security champions with cost-benefit analysis

9.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

- 4 Risk assessment and treatment
  - 4.1 Assessing security risks

9.3. Audience

The security coordination activity will need to commission an internal audit of the risks to the organisation's assets. If you have a formal management system in place, you may be able to appoint internal auditors to this task. The breadth of the investigation is an opportunity to involve more staff in the initial work of the ISMS and get their buy-in to the measures for protecting those assets they work with.

9.4. Deliverables

A comprehensive table of threats and risk that identifies where these risks must be controlled in the current set up. Then the gaps and inadequacies in the current security set up can be presented to the security coordination activity with cost benefit analysis.

- Comprehensive table of threats and risks to identify where risks must be controlled
- Gaps and inadequacies in the current security set up
- The role of the security expert
- Make initial judgements
- Balance conflicting opinions

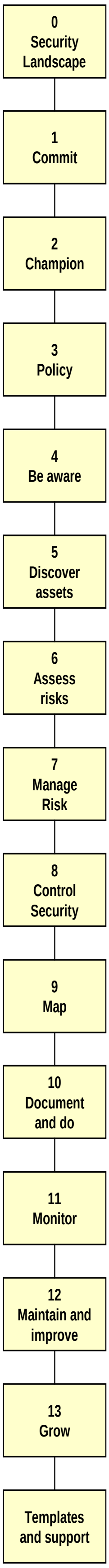
9.5. Successful techniques

Step one is 'analysis', there's no getting away from it, but it needn't cost huge consultancy fees. Step one is all about thinking about what may stop you delivering on time, getting the customer's order right, putting more money into your bank account than you're taking out. So, make a list, or get your staff to make a list of issues. Don't worry about completeness the first time through - experience and memory will help you add to your list with time.

Now look at what you've listed and consider how likely each showstopper or stumbling block is to crop up? Think about what will be the impact on your business if it does? Add these details to your list - make a table - now you can prioritise. All risks are bad but some are worse than others. You can prioritise. What will have the biggest impact and what is most likely to happen. Figure 11 shows you how to capture this information in an organised table.

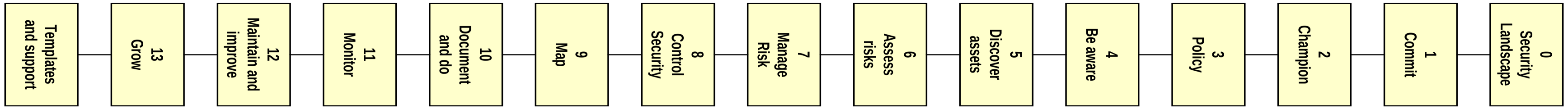
On the basis that the most valuable asset scores top mark of 5, and if the risk of losing its desired confidentiality, integrity, and availability is up to a mark of 5, and that an event which causes that to happen gets 5 if it's very likely, means that you've got a real problem! So in our model the worst mark - is 125/125 . . . 100%. The more you do to mitigate a risk, the less likely it becomes and so the probability score comes down. If you have good plans in place you can mitigate its effects and so the impact score comes down.

Now - time, memory, *and imagination* permitting - you will have a list of your major business risks.



				Initial assessment						Assessment after treatment		
Number	Information Asset	Information Owner	Importance of Asset	Risk Events	Probability of occurrence	Risk severity	Exposure or impact	Treatment strategy	Trigger date	Treated probability of occurrence (should be reduced)	Treated risk severity (should be same or less)	Residual risk exposure or impact
	Define this in words	Organisational role	Use 1 - 5 (1=low, 5=high)	Define this in words	How likely is this risk to occur? Use 1- 5 (1=low, 5=high)	How severe a problem is this risk if it occurs? Use 1- 5 (1=low, 5=high)	Multiply importance, probability and severity together, to derive a joint value	What are you going to do about this risk? □ Prevention □ Reduction □ Transference □ Contingency □ Acceptance	Controls to implement your risk treatment strategy.	Is this risk still likely to occur after treatment? Use 1- 5 (1=low, 5=high)	Will this risk still be as severe a problem if it occurs after treatment? Use 1- 5 (1=low, 5=high)	What is the expected risk after treatment has been implemented?
1	Database	Org.'s DBA	4	Deletion of key records	3.0	5.0	48%	Contingency: back up	01 January 2012	1.0	5.0	16%
2	Street Hardware	Local Authority	2	Vandalism	4.0	3.0	19%	Accetpance - monitor and replace	In place already	4.0	3.0	19%
3	Operator Logs	DIAMOND Sys. Admin	3	Editing	2.0	5.0	24%	Prevention: strong authentication and authorisation privileges	14 December 2011	3.0	3.0	22%
4	Speeding Tickets	Local Authority	5	Sent to wrong address	2.0	3.0	24%	Prevention with checking addresses; Transference of delivery to registered post	28 February 2012	1.0	3.0	12%
						Risk Factor	24%				Risk Factor	18%

Figure 11: A risk assessment and treatment template

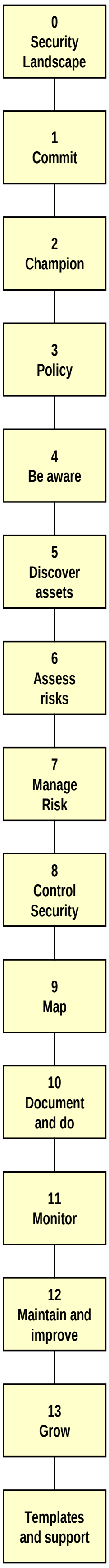


Your options are: prevent the risk - stop it happening; reduce the risk - reduce the impact if it does happen; transfer the mitigation of the risk - make it someone else's problem: this doesn't just mean outsourcing! Then there's contingency - because it is so likely to happen, be prepared! Finally there's acceptance of the risk. Some risks you will have to accept - it's unlikely that you'll be able to double up all staff skills and competencies etc. and will doubling up be enough? Where does it end?

The icing on your risk management cake is to assign trigger dates by which you will set the mitigation plans in place. This, with the mitigation plan (What are you going to do about this risk?) gives you point of control and reduces the surprises. Finally, remember to manage change and introduce review dates when you will check that your mitigation plans are still up to date and appropriate. With these ticking over, you can have the assurance that you are doing your best while you otherwise get on with the business. Once you get used to it, managing the risks - or even taking the risks - becomes one with the business.

9.5.1. The role of the security expert during this stage of the project

The problem with risk assessment is often not that of starting but rather stopping. An external view can help you steer your assessment within realistic boundaries. As you get more and more experienced your judgements as to the scoring of the risks and impacts will get better and better. Your security expert can help you make these initial judgements to get started and also take advantage of the independence to balance conflicting opinions as to whose assets need the most attention.



10. Stage 7 - Plan How to Reduce Risk to an Acceptable Level

10.1. Purpose

Now that you have identified the risks, you need to decide what to mitigate their impact (or make the business decision to live with them). Your options for risk management are based on a cost benefit analysis of various options available to handle the risk

10.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

- 4 Risk assessment and treatment
  - 4.2 Treating security risks
- 14 Business continuity management
- 14.1 Information security aspects of business continuity management
  - 14.1.1 Including information security in the business continuity management process
  - 14.1.2 Business continuity and risk assessment
  - 14.1.3 Developing and implementing continuity plans including information security
  - 14.1.4 Business continuity planning framework
  - 14.1.5 Testing, maintaining and re-assessing business continuity plans

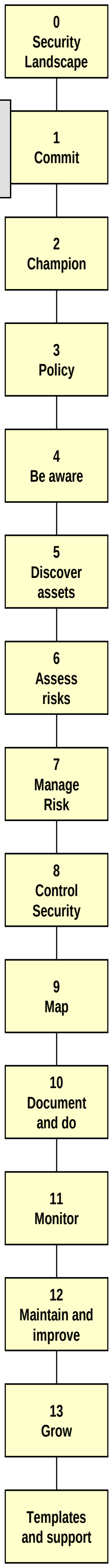
10.3. Audience

This is another of those areas that will touch almost everyone. The practical awareness of security issues will be raised during the audit process that identifies the risks to the organisation's information assets. Just as important is this opportunity to get the buy-in of staff in the mitigation processes (defined in the detailed policies of the statement of controls and their realisation through the documented processes and procedures) to ensure that the risk management processes are achievable.

10.4. Deliverables

This stage delivers a risk treatment plan and a corresponding business continuity plan[72]. The risk treatment plan defines:

- The level of acceptable risk in the organisation so that action can be taken to:
  - Accept risk once it is measured and understood to be within limits
  - Sign off risks that exceed the acceptable level depending on careful deliberation as to whether that is a risk to be taken
- When to transfer the mitigation of the risk, for example to a third party (such as the owner of a rented property being responsible for window grilles)
  - The plan shows that the risk is understood
  - Authorisation to transfer the risk mitigation is given



[72] As you will be considering the risks and bearing their treatment in mind, you will also be thinking of what is important to your operations. This is therefore an ideal time to determine the priorities of business continuity including for example, the minimum staff required for an acceptable level of delivery or service, essential equipment, premises, and so on.

- When to mitigate risk; this is when the control objectives and controls of ISO/IEC 27002 are applied. The plan will define:
  - Who is responsible for mitigating the risk
  - How the control is implemented

10.5. Successful techniques

10.5.1. Risk treatment

Consider what can you afford to do to stop the potential stoppers? This is the positive bit - risk mitigation.

Look at each risk and consider what is likely to stop it happening? This is an opportunity for you to involve the worriers and get them to do something positive. One of the key, background thoughts is to think about how much you might spend and how much the risk would cost to put right if it occurred. Remember not to spend thousands to protect an asset that would only cost hundreds to restore or replace. Keep this in mind; it helps you to keep your plans in perspective.

There are many fine software tools that may be acquired to record and monitor the management and treatment of risks. One of these should be considered although you may find that a simple spreadsheet that builds up your risk assessment will suffice (see Figure 11).

As to what to do with the risks the choice is:

Acceptance of the risk: You are aware of the risk but the solution to avoid the risk is too costly. You decide to live with the risk and face the consequences – a business decision.

Prevention or avoidance of the risk: For example, if there is an old server, which is malfunctioning, replacing it will avoid all the associated risk.

Mitigate the risk: Fully counteract the likelihood and/or impact of risks the risk. For example, stop illegal copying of software by restricting access to floppy and CD drives.

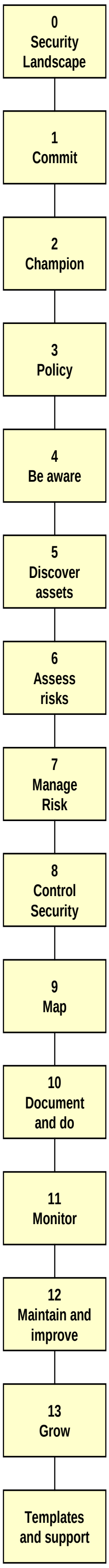
Risk reduction: You decide to take the bull by the horns and plan to identify the security measures, which will reduce the risk to an acceptable level or reduce the effect when it occurs.

Transfer the mitigation of the risk: For example, take a fire insurance policy and transfer the cost of the risk in the event of a fire to an insurance company. Bluntly, you make it somebody else’s problem.

This is the time to link your budget, business continuity plan, and risk treatment process together. Maintain consistency wherein your business continuity plan addresses the risks identified and your budgeting process allocates sufficient resources to implement the plans precautions.

ISO/IEC 27002 lists 135 general controls, which can be deployed to reduce the risk. Selection of specific controls should be based on the risk assessment carried out above. Select and implement policies that fit your appetite for risk. Consider:

- Secondary equipment, premises, understudying, or reciprocal arrangements with suppliers, partners, or even customers, for business continuity.
- User awareness as an effective and proactive tool in the defence against risk realisation
- Software asset management for cost effective licensing and the ability to make sure that you know where vulnerabilities need patching.
- An objective of **deperimeterisation** so that commensurate security arrangements are delivered where they are needed – not too much or worse . . .



- A general culture of hiding the maximum information from unwanted attention to make the implementation of security measures an integrated part of business processes, not an afterthought. Separate authentication from authorisation.
- Limiting access to just what is needed, and technical policies on the basis of 'if you don't need it . . . turn it off'.

Select each control through a cost vs. benefit analysis. Check whether cost of implementation of control is more than the risk we are attempting to reduce. For example, if you have to select the access control device for a location, controls range from simple swipe cards to biometric devices like retina scanners. Base your selection on the C-I-A rating of the objects you are trying to protect and the business impact of the security compromise. Take a judicious decision and select the control whose cost is less than the risk it is attempting to reduce.

10.5.2. The balance of risk treatment and business continuity

The day to day management of your business should contain risk within acceptable levels. This is what you have an ISMS for. However, the standards provide you with a realistic framework that recognises that there will be occasions when the threats are realised and the risk exceeds that acceptable level. When that level of risk is exceeded, the business continuity of your organisation is threatened. Business continuity should reflect the priorities that you show in the amount of risk you accept. When you plan for business continuity, you will be carrying out a 'sense check of your risk treatment – ask yourself whether you deployed controls according to your business priorities? Your recovery from security incidents should be a measured test of those plans and an opportunity to see if your expectations were met. Acting on what you learnt completes the virtuous circle.

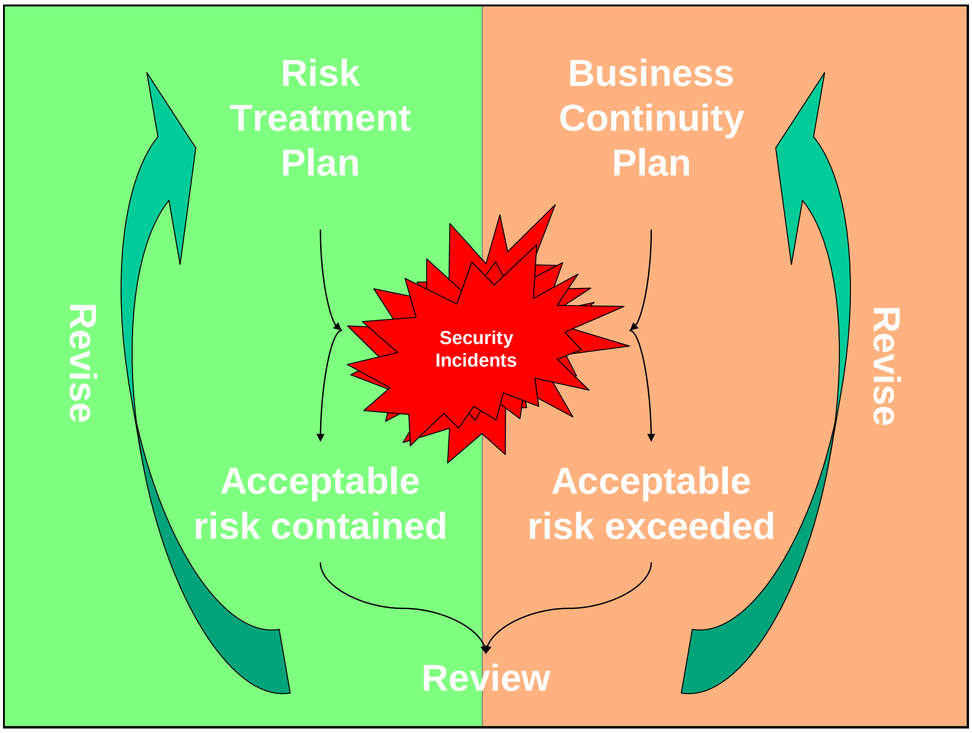


Figure 12: Containing risk within acceptable levels

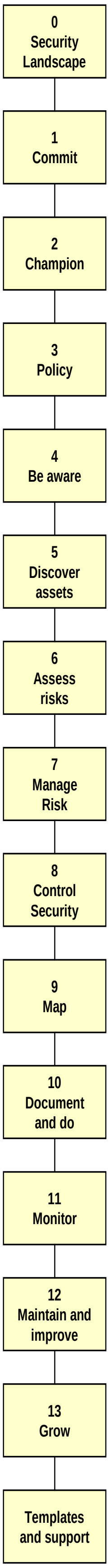
10.5.3. Business continuity management

10.5.3.1. Planning

If you haven't got one, a tested business continuity plan, consider that statistics from the University of Texas reveal that of companies suffering a catastrophic data loss, 43 per cent never re-opened and 51 per cent closed within two years. Only 6 per cent survived. Risk conjures up images of fire, flooding

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

or now, more so than ever, bombing, but it is far more common for telephone lines to fail, servers to crash, or for a local builder to cut through the mains electricity with a digger. And then there's the fifth column. Look not to the hacker but to the carelessness of your own staff or the maliciousness of an ex-employee. No wonder that there is talk not just of selecting technological controls but also building a human firewall too. The foundations for this are going be deep rooted. Current European Proposals point to education in 'respect for information' to begin at school level. There is no horizon to be avoided in countering risk.



The business continuity plan is such an important document that the process it encompasses warrants a complete section of the ISMS standard so it is worthwhile looking at it here in more detail. The process of business continuity is outside the scope of this chapter but you will need to understand what to put in your plan and so the contents are described here.

Use the plan to describe the strategy and guidance needed to ensure that the organisation is able to continue to satisfy the expectations of its mission in the event of disruption to the normal running of its infrastructure. It will probably focus on - but should not be restricted to - maintaining appropriate levels of information technology (IT) services.

The information will probably be unable to pre-empt every eventuality but rather provide a framework of tools, contacts and personnel who have the capability to provide office and IT services for the organisation. It is about the probability of incidents and the analysis and action based on the likely degree of impact and so fits hand in glove with the risk treatment plan.

Define in the plan the correct sequence of action to track the reaction of the 'Disaster recovery team' (see below) from the beginning of an event to having compromised and interrupted systems and activities up and running again.

Lay out the plan in such a way that it should be easy to use in an emergency situation to facilitate initial recovery, and a controlled return of the IT services and customer services to normal.

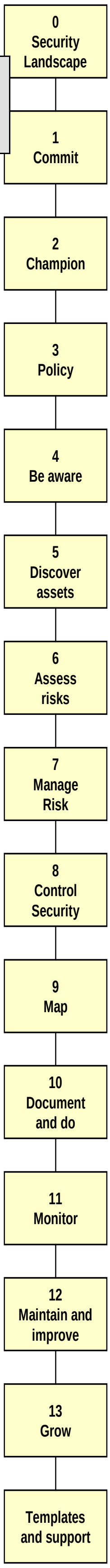
10.6. The role of the security expert

Every risk treatment plan should have the words 'don't panic' on the cover for encouragement. The treatment of risk is not a call sign for filling a cornucopia with expensive security technologies. It is the opportunity to recognise that the best technology has its weakest link in the way in which it is deployed. Use your security expert to facilitate a pragmatic approach to risk treatment based on the nature of your business, the cultures within your organisation, and the technical and social controls that you can afford.

11. Stage 8 - Establish Pragmatic Security Policies

11.1. Purpose

Compile a catalogue of policies (AKA policies document, statement of controls, or security manual) that will be the benchmark for decision making. This stage is where you develop the nitty gritty, day-to-day rules that realise the objectives of your high level security policy.



11.2. Audience

The rules will apply to all staff and contractors in the organisation but the methods of communication will vary. For example the format of passwords will be defined here but may be implemented by the network and users 'forced' into compliance (for example with dialogue to change a password after 60 days) rather than be presented with the textual rules from the control measures document.

11.3. Deliverables

This is where you develop the statement of security controls (detailed security policies) required to match the business of the organisation. This is where risk reduction starts. Your security policy statement (described in above) shows management commitment to information assurance. Detailed security policy statements define the operational level commitment to tackle each of the security risks identified during the threat and risk assessment. For example, if e-mail is recognised as a business critical function, every risk to your e-mail system as well as the threats that could be carried out by using the e-mail system will be addressed by an ‘E-mail security policy’. This policy should cover the organisation’s concern, approach to tackle the security issue and compliance requirements ranging from the misuse of e-mail to transmitting sensitive information to libelling colleagues or competitors.

Sample policies should be explained as part of the training and awareness programme.

11.4. Successful techniques

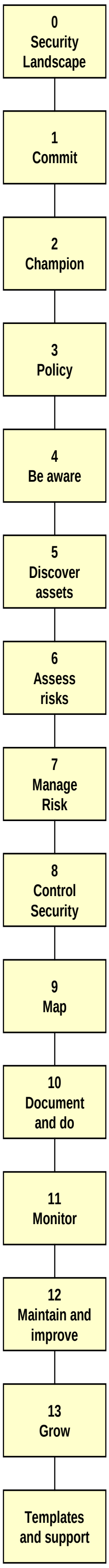
11.4.1. ‘Pick and mix’

See your security policy as a high level document and this statement of controls as the detailed policies. Associate the controls (or policies) with your risk assessment and business continuity plan so that you introduce controls that support them. Don't adopt controls that you do not need - your control for the insecurity of wireless networks may be not to use wireless technology. You may need to use it in which case a suitable method of encryption would need to be deployed and your statement of controls would specify the requirements for it. This can then be reviewed in the light of new technology or security incidents to make sure that the control or policy is kept up to date and effective. You will need policies to control activities relevant to your organisation. The following list is neither exhaustive nor comprehensive but will give some idea of what you may need to pick and mix[73]:

- New installations and change management procedures
- Firewall configuration
- Router configuration
- Internet access plan
  - General organisation’s Internet DMZ
- General configuration
- Demonstration facility and lab security
- Equipment outsourced to external service providers
- Wireless communication
- Server security

[73] For a really comprehensive list see the Policies Project at www.sans.org

  - Secured hosted Internet DMZ
  - Open hosted Internet DMZ
  - Internal organisation’s subnet
  - Organisation’s Internet DMZ equipment
  - Secure hosted Internet DMZ equipment
  - Equipment outsourced to external service providers
  - Open hosted Internet DMZ equipment
- Remote access
- Data backup
- System administration
- Disposal of computer equipment
- Audit
- Monitoring
- Compliance
- Data access
  - New starter data access
  - Data access for leavers
  - Data access modifications
- Passwords
- Virus protection procedure
- Acceptable use of computers
- Removal of computer equipment
- Data protection
- Intellectual property



Include the purpose and scope of each policy, and how you enforce it, or deal with policy breaches, in your definitions.

Security policy cannot always be implemented just by having well defined administrative procedures. It may be necessary to select some products to implement some of the clauses of security policy. For example e-mail security policy may state that the user should not use profane, obscene language in the email. Only a device like content filter could detect violation of this policy by users. Identify security management and control products but never lose sight of the policies you are fulfilling by implementing technology.

11.5. The role of the security expert

The strength of the ISO/IEC 27001 and ISO/IEC 27002 combination is its risk-based approach that allows you implement controls commensurate with circumstances and accept risk at justifiable levels. It is often tempting as an insider to either take on too much or be pressurised into implementing too little. The security expert can help you to match the right physical and logical controls to protect the relevant assets from the potential threats. This starts with the mitigation measures of the risk treatment plan and extends to the statement of controls which defines the detailed policies to protect your information assets. This can then be audited for completeness and a statement of applicability[74] created.

[74] See the next section and the template included in the appendix.

12. Stage 9 - Map Out Where Your Security Controls Should Be

12.1. Purpose

So far, you have taken the risk management approach for identifying and mitigating the risks. Now check your selection of controls against the 135 controls defined by ISO/IEC 27002. As explained, these controls are described in very general terms and no specific interpretation has been provided. The emphasis is on the selection of appropriate controls based on the risk assessment. This will create a statement of applicability which matches the business of your organisation. (When you check that the controls are in place then your statement of applicability will become your first internal audit of your ISMS.)

12.2. Audience

Security officer/coordinator (or a perhaps a panel of representatives in larger organisations) show the completeness of measures taken and it will be assessed for completeness during any third party certification.

12.3. Deliverables

A statement of applicability showing which of the 135 from ISO/IEC 27002 controls are used to manage risk throughout your organisation. It will also list:

- Additional controls and the reason for their selection.
- Excluded controls and the justification for not applying them.

12.4. Successful techniques

Tabulate the controls from Appendix A of ISO/IEC 27001 and check that you applied appropriate controls to right processes and places. This is a good gap analysis of your compliance with the standard and needs to be revisited regularly. Include it on your schedule of internal audits.

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
9.1.1 Physical security perimeter	Reception Locked doors to: · Premises · Computer room		Key fobs and ID cards Reception of Visitors process Raised flooring divided by wall from outer corridor.	Careful attention paid to security during refurbishment	Alarms under review

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
9.1.2 Physical entry controls	Fob entry to secure areas limited to named staff. Areas out of bound to public clearly marked and controlled by staff vigilance.		ID fobs and notices. Reception of Visitors process List of authorised personnel and access granted by fobs. Keypads for higher risk areas	New risk assessment done as a result of planned refurbishment .	
11.7.2 Teleworking	Homeworker, ad hoc sales team access and management access.		Risk assessment performed. Access controlled through secure password system. VPN used by staff working remote via broadband	Risk reduced; less teleworking.	

Table 4: Sample from a statement of applicability[75]

12.4.1. Check which ISO/IEC 27002 controls you have in place

Create a statement of applicability as an audit of the completeness of your ISMS. Make a table of all the 135 controls and map the controls implemented by you against relevant ISO/IEC 27002 control objectives and controls. One implemented control may address more than one ISO/IEC 27002 control. Review your statement of controls whenever significant changes take place – such as introducing wireless technology where none was used before. As a rule of thumb, make a full review every six months to pick up all the small improvements and changes that you will most likely have made to your ISMS.

12.4.2. Identify the gaps between what's in place and what should be

If there are some gaps, find out, whether these are unintentional omissions or there are no requirements of controls. Recheck the evaluation of risks and threats performed by you. Validate the business risk analysis performed earlier. You may be able to justify the gap if the risk assessment has not shown requirement for a particular control. If so, explain the reasons for exclusion as part of the statement of applicability. Give the risk assessment reference, which will support your statement.

12.5. The role of the security expert

As before, the greatest advantage of the security expert is the fresh pair of eyes and here that independent view can help you assess the completeness of your controls – have the controls been applied in **all** applicable areas?

[75] A complete template for a statement of applicability is included as an appendix to this guide.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

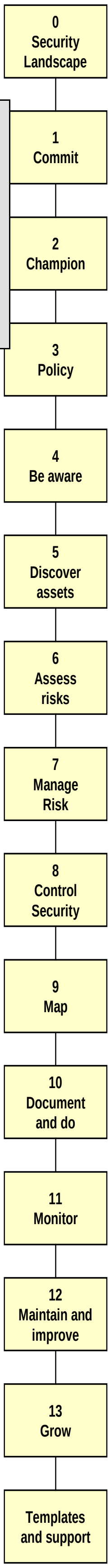
13. Stage 10 - Write and Implement Your System Security Plans, Processes, and Procedures

13.1. Purpose

Each policy in the statement of controls will be supported by appropriate plans, processes, procedures, instructions and guidelines based on selected practices and, in some instances, products.

Note: Many documented processes will cover several policies or parts of policies. Don't tie your ISMS in knots by trying to maintain a 1:1 relationship between policy and procedure . . . although you must be able to map one on to the other (and it will probably be apparent in your statement of applicability).

The procedures should be detailed and unambiguous enough for every person to follow. These will explain how to assure the security of the business.



13.2. Audience

The whole organisation will be touched by one or more plans or procedures and so the level of detail will have to vary depending on the level of training and experience of the staff. This is a key point. The purpose of the documentation is to convey information at the right level. Your ISMS is a combination of people, resources and processes. The documentation is not designed to enable you to run the organisation by numbers - a well-documented procedure for setting up firewall software is for suitably experienced staff, not for an inexperienced trainee or someone from a completely different discipline.

13.3. Deliverables

Defined procedures:	Procedures define details regarding implementation of the security policy. These will provide details like responsibilities of various groups, actions to be taken for preventing, detecting, correcting and reporting security lapses.
Defined standards:	The organisation may decide to follow some international standards in the area of information security. For example, for e-mail security, the organisation may select S/MIME as the standard for secure e-mail exchange.

13.4. Where does it get you with ISO/IEC 27001 compliance?

A long list of sections referenced here because this is where you will develop reliable, repeatable business processes that may be lacking – or need improvement - in your organisation. This stage is designed to address the following controls selected from ISO/IEC 27002 processes for:

8 Human resources security	11 Access control
· 8.1 Prior to employment – 8.1.1 Roles and responsibilities – 8.1.2 Screening – 8.1.3 Terms and conditions of employment · 8.2 During employment – 8.2.1 Management responsibilities – 8.2.2 Information security awareness, education and training	· 11.1 Business requirement for access control – 11.1.1 Access control policy · 11.2 User access management – 11.2.1 User registration – 11.2.2 Privilege management – 11.2.3 User password management – 11.2.4 Review of user access rights · 11.3 User responsibilities

    - 8.2.3 Disciplinary process
- 8.3 Termination or change of employment
    - 8.3.1 Termination responsibilities
    - 8.3.2 Return of assets
    - 8.3.3 Removal of access rights

9 Physical and environmental security

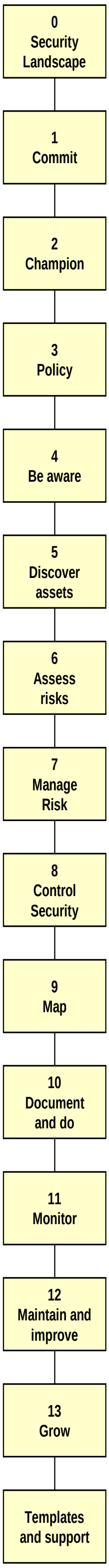
- 9.1 Secure areas
    - 9.1.1 Physical security perimeter
    - 9.1.2 Physical entry controls
    - 9.1.3 Securing offices, rooms and facilities
    - 9.1.4 Protecting against external and environmental threats
    - 9.1.5 Working in secure areas
    - 9.1.6 Public access, delivery and loading areas
- 9.2 Equipment security
    - 9.2.1 Equipment siting and protection
    - 9.2.2 Supporting utilities
    - 9.2.3 Cabling security
    - 9.2.4 Equipment maintenance
    - 9.2.5 Security of equipment off-premises
    - 9.2.6 Secure disposal or re-use of equipment
    - 9.2.7 Removal of property

10 Communications and operations management

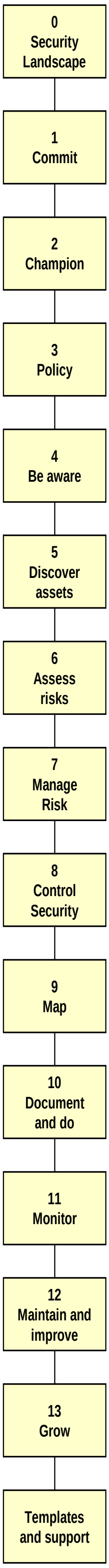
- 10.1 Operational procedures and responsibilities
    - 10.1.1 Documented operating procedures
    - 10.1.2 Change management
    - 10.1.3 Segregation of duties
    - 10.1.4 Separation of development, test and operational facilities
- 10.2 Third party service delivery management
    - 10.2.1 Service delivery
    - 10.2.2 Monitoring and review of third
    - 11.3.1 Password use
    - 11.3.2 Unattended user equipment
    - 11.3.3 Clear desk and clear screen policy
- 11.4 Network access control
    - 11.4.1 Policy on use of network services
    - 11.4.2 User authentication for external connections
    - 11.4.3 Equipment identification in the network
    - 11.4.4 Remote diagnostic and configuration port protection
    - 11.4.5 Segregation in networks
    - 11.4.6 Network connection control
    - 11.4.7 Network routing control
- 11.5 Operating system access control
    - 11.5.1 Secure log-on procedures
    - 11.5.2 User identification and authentication
    - 11.5.3 Password management system
    - 11.5.4 Use of system utilities
    - 11.5.5 Session time-out
    - 11.5.6 Limitation of connection time
- 11.6 Application and information access control
    - 11.6.1 Information access restriction
    - 11.6.2 Sensitive system isolation
- 11.7 Mobile computing and teleworking
    - 11.7.1 Mobile computing and communications
    - 11.7.2 Teleworking

12 Information systems acquisition, development and maintenance

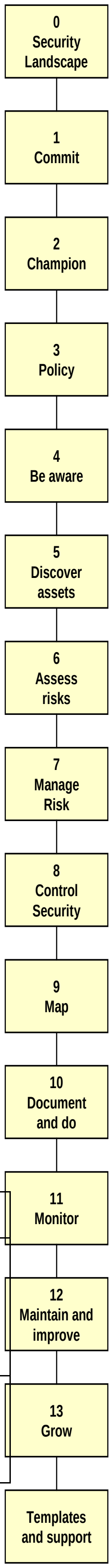
- 12.1 Security requirements of information systems
    - 12.1.1 Security requirements analysis and specification
- 12.2 Correct processing in applications



  - party services
  - 10.2.3 Managing changes to third party services
- 10.3 System planning and acceptance
  - 10.3.1 Capacity management
  - 10.3.2 System acceptance
- 10.4 Protection against malicious and mobile code
  - 10.4.1 Controls against malicious code
  - 10.4.2 Controls against mobile code
- 10.5 Back-up
  - 10.5.1 Information back-up
- 10.6 Network security management
  - 710.6.1 Network controls
  - 10.6.2 Security of network services
- 10.7 Media handling
  - 10.7.1 Management of removable computer media
  - 10.7.2 Disposal of media
  - 10.7.3 Information handling procedures
  - 10.7.4 Security of system documentation
- 10.8 Exchanges of information
  - 10.8.1 Information exchange policies and procedures
  - 10.8.2 Exchange agreements
  - 10.8.3 Physical media in transit
  - 10.8.4 Electronic messaging
  - 10.8.5 Business information systems
- 10.9 Electronic commerce services
  - 10.9.1 Electronic commerce
  - 10.9.2 On-Line Transactions
  - 10.9.3 Publicly available information
- 10.10 Monitoring
  - 10.10.1 Audit logging
  - 10.10.2 Monitoring system use
  - 10.10.3 Protection of log information
  - 12.2.1 Input data validation
  - 12.2.2 Control of internal processing
  - 12.2.3 Message integrity
  - 12.2.4 Output data validation
- 12.3 Cryptographic controls
  - 12.3.1 Policy on the use of cryptographic controls
  - 12.3.2 Key management
- 12.4 Security of system files
  - 12.4.1 Control of operational software
  - 12.4.2 Protection of system test data
  - 12.4.3 Access control to program source code
- 12.5 Security in development and support processes
  - 12.5.1 Change control procedures
  - 12.5.2 Technical review of applications after operating system changes
  - 12.5.3 Restrictions on changes to software packages
  - 12.5.4 Information leakage
  - 12.5.5 Outsourced software development
- 12.6 Vulnerability management
  - 12.6.1 Control of vulnerabilities



– 10.10.4 Administrator and operator logs – 10.10.5 Fault logging – 10.10.6 Clock synchronization	



13.5. Successful techniques

Hard work! There are no short cuts to:

- Writing security management processes and procedures
- Implementing and using the processes and procedures

But documentation is all about managing risk – balancing the tacit expertise with the need to set out what is expected of staff. This is of course is not a job that you will do alone. You must call on the suitably experienced to write the first full draft of any procedure and have the version to be issued signed off by an appropriate authority. Here we look at making documentation easy to use and suggest an efficient way of writing it.

13.5.1. Avoiding too much documentation: keeping it simple and effective

13.5.1.1. The role and purpose of processes and procedures

Processes and procedures are all about verbs; they are about doing things. Procedures should tell you what to do, how to do it, when to do it and why you are doing it. Everyone in your organisation is responsible for the security of his or her work. It is not enough to say to someone follow the policy. Policies are goals and aspirations to be achieved. How can they be expected to know what your definition of 'security' is? How can they find out what they have to do to achieve it? And how can they tell whether their work is acceptable?

Documented processes and procedures remove this uncertainty, because:

- They define the practical things you must do to achieve a secure result
- They provide confidence that work carried out according to the processes and procedures will contained with acceptable levels of risk.

Processes and procedures ensure consistency of results. If everyone with the right competencies and skills follow the same processes and procedure, they will be doing things in the same way. You will be able to depend more on the work of others when it is passed on to you. There will be fewer unpleasant surprises. You can also shorten the learning curve for the newcomer

13.5.1.2. A simple format for documentation

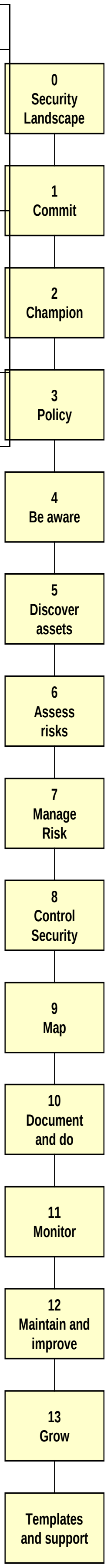
Document processes and procedures in an **E**ntry-**T**ask-**V**erification-e**X**it format[76] covering:

Section	Contents
Process objectives	Describe briefly what the process intends to achieve, to whom this procedure applies, who is not permitted to carry out the tasks or functions, who keeps the process up-to-date, and who owns/authorises the procedures.
Entry criteria	Define whatever it is that starts this process (Is it a calendar based event? Is it the result of a security incident? Can it only be started if the top management approves it? etc.)

[76] This was created by IBM as a programming template. We've used it a systems template in the wider sense. See the example in the appendix.

Section	Contents
Tasks to be carried out	Write down a list of ‘to do’s’ that are essential to the task being carried out. Include the responsibilities - can this be done by anyone or must it be done by someone in particular (such as a director, a head of section, accountant, personnel, project manager). Note that the level of detail here is linked to the competency of staff involved.
Verification criteria/activities	Set out what has to be done to make sure that everything to do with this process is running smoothly. E.g. Who has authority to sign-off the business continuity plan? Who checks the technical accuracy? Who checks the release of intellectual property into the public domain?
Exit criteria	Be specific about the activities that denote the end of the process. Does it kick-start another?

Table 5: Process/procedure definition: the contents



Some security policies and their supporting documents have a consistent failing, and that is a tendency towards ambiguity with the requirement levels. Documents say that an action ‘should’ be taken when they mean it ‘must’ be taken; they say that staff ‘may’ perform an action when they really mean that the action ‘should’ be performed.

A simple, authoritative guide to clarity in this field is Internet Engineering Task Force’s RFC2119[77].

This document is a formal specification for the meanings of ‘must’, ‘must not’, ‘required’, ‘shall’, ‘shall not”, ‘should’, ‘should not’, ‘recommended’, ‘may’ and ‘optional’. Its definitions are clear, unambiguous and concise. Those tasked with writing policy, standard or procedure documents will find it useful, and it should certainly be included as an appendix to all such documents. Care needs to be taken when writing the documents that the words listed above are used in a manner compliant with the RFC.

13.5.1.3. The Ownership of Procedures

A word of warning! If the ownership of a process is at too high a level (for an extreme example, take the Managing Director) there is a risk that it will not be changed or not reflect the real 'shop floor' practice. Operational staff will be reluctant to challenge or follow it. Don't let the definition of processes get too high. Managing Directors should set policy not process. Select the appropriate level of ownership for each process and procedure. A local manager may be required for approval, but make sure that those who actually carry out the task have a say in the formulation of the procedure (the written definition of that task).

13.5.1.4. Roles

The first step to make is that of recognition. You must recognise that the ISMS needs to be flexible. If you align the documentation of the ISMS according to the structure of the organisation, the ISMS may breakdown if you reorganise. At the very least, you will be faced with the possibility of considerable work to bring your documentation into line with the changes.

So the first task in planning your processes and procedures is to separate the structure of the organisation from what the organisation does. The key word is function. The organisation of the company, however complex or fluid, can be contained in one short document. What your organisation needs to do in terms securing its information during the manufacturing of materials, running SCADA[78]

[77] www.ietf.org/rfc/rfc2119.txt

[78] **S**upervisory **C**ontrol and **D**ata **A**cquisition

systems, developing hardware or software or supplying services will need far more words and but will be less changeable than you think.

Refer to roles rather than job titles. Your organisation is probably far less hierarchical when it comes down to getting the job done. Procedures must be operational within this flatter structure to take account of the various roles that an individual may take on during the course of a process.

13.5.2. Quality control for processes

No matter how good your procedure is, there will be someone somewhere who will not accept it until they have had the opportunity to comment on it. The review of a procedure is essential (and this also applies to modifications to existing procedures). Of course we must keep this in perspective. Do not call a review meeting if you have just altered the wording to make something clearer or correct a spelling mistake.

13.5.2.1. Validating processes

There are several different ways of validating processes. These range from Fagan inspection to 'suck it and see'.

The 'suck it and see' is the least satisfactory method and is usually coupled with the misuse of internal audits. The internal audit is not meant to provide guidance about the correctness of a security control (although this may be a by-product of the process). The purpose of the internal audit system is one of verification. They should be run to monitor conformance to both the documented ISMS in operation and to the requirements of the ISO/IEC 27001 standard. The system provides the mechanism for discovering non-conformances within the operating ISMS, ensuring that appropriate corrective action is planned, implemented and effective. Day-to-day carrying out of processes should be helped by training (once a procedure is in place). Don’t rely on the internal audit system to 'test' processes; that is like waiting for system testing to identify fundamental design flaws in the software.

This said, do not wait for perfection. Issue usable processes and improve them with time. Withhold them until every last detail is sorted out and you can issue them to find that the goal posts have moved and the processes do not meet their objectives.

A simple but effective approach involves three stages:

- Preparing to review the procedure
- Reviewing the procedure
- Completing or reworking the procedure

13.5.2.2. Preparing to review the procedure

Select a team of reviewers. Ask them to review a procedure from a particular point of view. Three possible aspects are described here:

- A technical review
- A usability review
- A business review

A technical review should determine whether the procedure specifies the correct activities in the correct sequence and that responsibilities are correctly assigned and consistent with the authority necessary to carry out the task.

A usability reviewer should decide whether the procedure is explicit enough that it can be used and is useful. It should also consider whether the activities specified can actually be performed.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Procedures may implicitly require resources to be available at certain times. The business review should consider whether both the implicit and explicit resources are likely to be available and the overhead this could add in terms of time and cost to the performance of the task.

To make the aspect to be reviewed clear to each reviewer, use checklists. Supply each reviewer with a copy of the procedure and a predefined checklist. Here are some examples of the type of questions that may be appropriate to each aspect.

A technical review checklist:

- Is the scope, as specified, appropriate?
- Does the procedure consider all the possible situations that can occur within the specified scope?
- Are the 'mechanics' of the procedure correct?
- Are any timescales mentioned feasible?

A usability review checklist:

- Is the level of detail appropriate to the task (bearing in mind who is responsible for performing the task)?
- Is it possible to perform the activities as specified?
- When strung together, do the activities form a coherent process?
- Are the roles described to an appropriate level of detail?
- Will this procedure be useful?
- Is it practical to implement for the prescribed scope?

A business review checklist:

- Is the approach taken in the document sufficient to minimise any business risks involved in this task?
- Is the procedure practical to implement from a resource, time taken and timescale point of view?

13.5.2.3. Reviewing the procedure

Essentially, there are three methods that you can use to review processes:

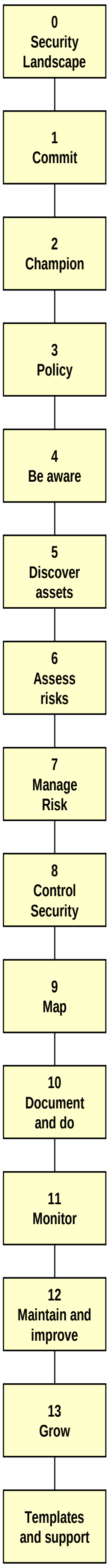
- Peer review or desk checking by one or more reviewers
- Review by informal meeting
- Formal documentation inspection or Fagan Inspection

In each type of review, reviewers should have a clear picture of their role and the time constraints of the review. Reviewers are also responsible for ensuring that they clearly communicate the results of their reviews.

These three methods represent three levels of review that vary from simple to formal. The level of review depends on:

- How important is the procedure?
- How capable and experienced is the author of the procedure?
- Does the procedure describe the interconnections between different functions?

The questions must be answered honestly. They must not be used to try to dilute the information assurance process.



13.5.2.4. Reworking or completing the procedure

The results of each review must be carefully considered and appropriate changes made. Where copious change results from a review, the procedure may have to be reviewed again. If a formal review technique was used for the initial review, a less formal method may suffice for the second or subsequent reviews. Give reviewers the opportunity to see changes wherever practical.

When the procedure is sound, make sure that it receives a review for language, typing and so on. A fact, strange but true, is that faith can be lost in an excellent procedure because of a few careless typographical errors. Typical questions for a proof reader are:

- Does the document conform to accepted housestyle?
- Is the document free from spelling mistakes?
- Is the document free from grammatical mistakes?
- Is the document free from any other typographical mistakes?

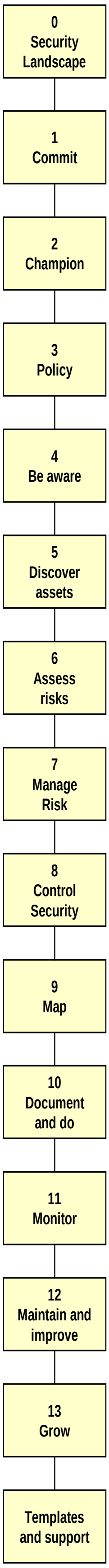
Review checklists are not afterthoughts. Use them when writing the first draft of the procedure.

13.6. The role of the security expert

This is where many organisations make a mistake with management systems; they believe that they can be created by a third party. Beware any ‘expert’ who offers to document the processes and write the processes for you. This will give you:

- A third party bias and not a third party view
- A lack of ownership for your ISMS will eventually affect you but will immediately affect your staff
- A set of ‘foreign’ documents which you will find unfamiliar and difficult to update

Use the expert to facilitate the documentation process, perhaps drafting skeleton documents for others to complete or to work alongside the process owners who have difficulty documenting their roles, responsibilities and actions. The expert can again take the third party view by helping you to resolve cross-department issues where mediation may be needed – not least when stringent countermeasures required for one department require equally stringent measures elsewhere as a knock-on effect.



14. Stage 11 - Monitor and Review the ISMS Performance

14.1. Purpose

The effectiveness of how you manage security incidents is a good measure of the effectiveness of your ISMS. What were the outcomes of incidents? If you exceeded the level of acceptable risk to particular assets, have you referred this to the asset owners to consider whether the levels must be reappraised? Is the level of risk increasing or decreasing? Do incidents invoke your business continuity plan?

As if the law is not encouragement enough, compliance with ISO/IEC 27001 requires that you monitor which laws apply to your business and comply with them. Include in your ISMS the processes required by laws and regulations. Your ISMS will provide a framework that will deliver compliance to many of the requirements of the statutes as a by-product of good business management.

The ISMS is not a marketing tool (although it can help); it is a serious, integrated part of your business processes required to assure the information that you handle. Implementing the ISMS is not a one-off job. Good governance demands that it needs to be constantly monitored and reviewed to make sure that it remains faithful to your business objectives.

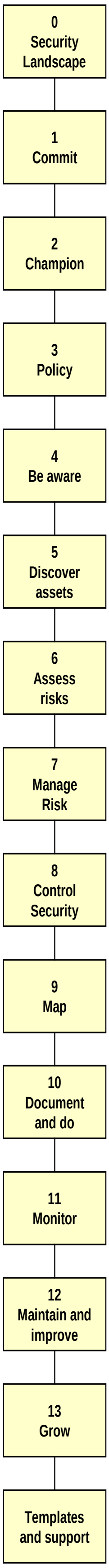
0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

14.2. Where does it get you with ISO/IEC 27001 compliance?

This stage is designed to address the following controls selected from ISO/IEC 27002:

13 Information security incident management	15 Compliance
· 13.1 Reporting information security events and weaknesses – 13.1.1 Reporting information security events – 13.1.2 Reporting security weaknesses · 13.2 Management of information security incidents and improvements – 13.2.1 Responsibilities and procedures – 13.2.2 Learning from information security incidents · 13.2.3 Collection of evidence	· 15.1 Compliance with legal requirements – 15.1.1 Identification of applicable legislation – 15.1.2 Intellectual property rights (IPR) – 15.1.3 Safeguarding of organizational records – 15.1.4 Data protection and privacy of personal information – 15.1.5 Prevention of misuse of information processing facilities – 15.1.6 Regulation of cryptographic controls · 15.2 Compliance with security policies and standards – 15.2.1 Compliance with security policy and standards – 15.2.2 Technical compliance checking · 15.3 Information systems audit considerations – 15.3.1 Information systems audit controls – 15.3.2 Protection of information

	systems audit tools



14.3. Who is the 'audience' for this stage of the project

Involve your business management team and the staff that you appointed in your 'security organisation'.

14.4. Deliverables

As a result of your monitoring and review processes, the checks that you will have in place will produce information that you can amalgamate into an action plan. This will ensure that you can track the necessary changes to your policies and implement new processes (and eliminate the redundant ones). This is a key stage of the plan-do-check-act lifecycle.

14.5. Successful techniques

14.5.1. Prioritising actions for improvement

Create an action plan that addresses the actions arising from security incidents, internal audits, and management reviews. This will give you a central, consistent focus on the improvements that you need to make and will help you to prioritise them.

14.5.2. Staying within the law

Laws and regulations provide the controls that we need to steer people and organisations through many of their social obligations. Rather than see these controls as restrictions, look upon them as supporting business. There is little that can be described as ‘IT Law’ but any business needs to be aware of laws that may have implications in the deployment of information systems. The following table may be daunting (not least in that it cannot be comprehensive – specialist regulations for the sectors in which the information systems are deployed must be respected). However, the plan-do-check-act approach of an ISMS that controls the confidentiality, integrity, and availability of information will do much for the organisation’s governance, keeping it compliant by meeting the expectations of these edicts.

Anti-terrorism	Basel II Accord, Civil Evidence Act 1968 and the Police and Criminal Evidence Act 1984
Civil Jurisdiction and Judgements Order 2001	Communications Act 2003
Companies (Audit Investigations and Community Enterprise) Act 2004	Computer Misuse Act 1990
Consumer Protection (Distance Selling) Regulations 2000	Copyright (Computer Programs) Regulations 1992
Copyright and Rights in Databases Regulations 1997[79]	Copyright etc. and Trade Marks (Offences and Enforcement) Act 2002
Crime and Security Act 2001	Cybercrime Convention 2001
Data Protection Act 1998	Disability Discrimination Act 1995
Electronic Commerce (EC Directive) Regulations 2002	Electronic Communications Act 2000

[79] Think about protecting your own intellectual property and the respect your show for that of others.

EU Framework Decision on attacks against information systems	Freedom of Information Act 2000
Human Rights Act 1998	Money Laundering Regulations 2003
Official Secrets Act 1989	PATRIOT Act 2001 (USA)
Privacy and Electronic Communications (EC Directive) Regulations 2003	Proceeds of Crime Act 2002
Public Records Acts 1958 and 1967	Sarbanes-Oxley Act 2002 (USA)
The Regulation of Investigatory Powers Act 2000	The Re-use of Public Sector Information Regulations 2005
The Value Added Tax (Amendment) (No. 6) Regulations 2003	Value Added Tax (Reverse Charge) (Amendment) Order 2003
Waste Electrical and Electronic Equipment Directive (2002/96/EC)	Wireless Telegraphy Act 1949

Table 6: Laws and regulations with IT implications

14.5.3. Other 'tools' for compliance

Consider other complementary frameworks that keep the check and balances for your information systems in place. For example:

- Do you use, or issue, digital signatures? tScheme sets out the standards to be met for the assurance of trust in those signatures
- The implications of representing certain types of business on the World Wide Web can be managed through codes of practice.
- CoBIT is an auditing regime maintained by the Information Systems Audit and Control Association. If ISO/IEC 27001 is the specification for an ISMS, CoBIT is its test plan.

14.5.4. Managing incidents

The test of an ISMS is not the eradication of security incidents. This is not achievable. It is how you deal with them. Is an incident a 'one-off' or is it endemic and recurring? These questions help you to prioritise your response.

One positive view of security incidents is to use them as tests of your ISMS or specifically your business continuity plan. So if your do have an interruption to and IT service, consider:

- Whether the service was recovered and restored within the targets you have set
- How much did it cost to restore the service
- Are your costs of dealing with incidents rising or falling?

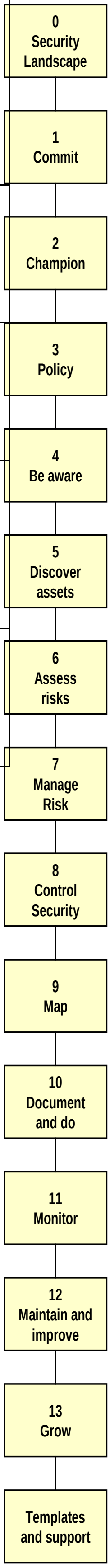
Review your internal audit schedule in the light of incidents. Have areas that you had planned to audit been adequately tested already by an incident? Amend your schedule; don't repeat what has now become unnecessary duplication.

14.5.5. Records for use, not for their own sake

Create the following mechanisms for effectively monitoring and reviewing the ISMS performance:

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Information	Use and content
Reporting system	Include: · Reporting security incidents · Reporting security weaknesses · Reporting software malfunctions
Fault logs	Each control can generate huge amounts of information. Ensure that this information is properly recorded and stored for analysis. Don't keep information for the sake of it; only analyse information that is useful to the organisation.
Review mechanism	The incident reports will be of no use if they are not reviewed regularly. The formation of security organisation should include assigning specific responsibilities to teams or individuals to periodically review the logs and reports.
Internal Audit	Periodic audits should be performed to review the performance of various controls and measures defined in ISMS. Internal audit teams or external consultants could perform the audit. The audit findings should be documented and all non- conformities must be corrected and reported within a specific time frame.
Management Review	The Security Steering Committee should conduct a management review of the performance of ISMS at least once a year. This review should be based on various reports submitted by incident reporting and review processes and internal audit reports.



14.5.6. Internal auditing

Internal audits help to steer day-to-day practice along the route maps of business plans. They test the effectiveness of previously applied measures. Internal auditing monitor conformance, to both the documented ISMS in operation and subsequently, to the requirements of any standards upon which the system is based.

Internal audit records form part of your management system records. From these records trends, critical problems, persistent problems and so on, can be identified. Third party assessors (also probably second party assessors) will examine these records. They will be looking to satisfy themselves that the non-conformances identified during internal audits have been cleared and that the internal audits themselves are operating effectively.

The internal audit function is the mechanism through which the operation of the ISMS is formally monitored and conformance with the documented ISMS is assured. Audits are carried out by auditors selected from within the company but who are independent of the area, function or procedure being audited.

Note: The approach to auditing will vary depending on the size and complexity of the organisation involved. It's still an internal audit system whether you make integrated checks through the business process or whether you have a team of auditors crossing sites checking compliance to the nitty gritty of security procedures.

Internal audits are the mechanism through which information about the effectiveness of the ISMS is gathered. The purpose of the audit function is to verify, or otherwise, conformance of practice with the documented ISMS and with the requirements of the Standard.

Very often this is seen as a policing function, so great care must be taken to promote the audit as a positive contribution to improvement. The nature of audits, of course, makes this difficult - recording non-conformances appears to be quite negative. However, where an effort is made to note positive aspects the overhead in time seems to be unsupportable. In other words, it is probably not practical (although it is not impossible) to introduce ‘positive’ auditing.

Some people do positively welcome audits as a rare opportunity to show off their day-to-day activities and have their successes visibly reported to management.

14.5.6.1. Types of audit: internal and external audits

There are three different types of audit:

- First party audits
- Second party audits
- Third party audits

The first party audit is the mechanism by which the company monitors adherence to the documented ISMS. It carries little weight externally, except as confirmation that the ISMS is operating correctly. Its benefit is to the company. It provides objective data used to highlight the potential for improvement and a basis on which to plan improvements. The audits are carried out by people who understand both the company and its activities.

Second party audits are usually performed by the customer, or a representative of the customer, when the customer needs to establish confidence in the processes contributing to a particular product or service.

Third party audits are performed by agencies, independent of both customer and supplier, recognised as competent to assess an ISMS against a standard. In recognition of meeting the requirements of the standard, the supplier will achieve certification to the standard. Certification has the benefit of reducing, if not completely removing, the need to perform second party audits.

14.5.6.2. The basic approaches to auditing

Within these three types of audits, there are two approaches that auditors can take:

- Vertical auditing
- Horizontal auditing

Vertical audits look, in depth, at a particular function or department. This type of audit would monitor the use of all relevant processes as they are used to support the function or activity. Internal audits are usually vertical audits.

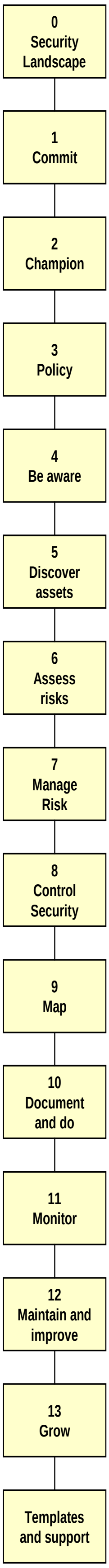
Horizontal audits follow a process from start to end. This type of audit would look at processes as they support the process itself and is likely to span many different functions or departments. Audits or assessments leading to certification are likely to be horizontal.

14.5.6.3. The structure of an internal audit system

The internal audit process is a documented system covering the planning, execution and follow-up of audits carried out within the scope of the ISMS. It is part of the ISMS itself.

A typical internal audit process will combine three functions:

- Management representative (usually the security coordinator)
- Internal auditors
- Management review body



All three of these elements are required but the method and style of construction of the internal audit process itself is not mandated. In practice, the internal audit process needs the support of a corrective action system to be effective.

Taking this model as a typical example, we now look at little more deeply into the function and role of each of these elements.

Let us now look in more detail at who is involved in Internal Audits.

14.5.6.4. Organising audits: management

Internal Audits, like the rest of an ISMS, require backing from the organisation’s top management. This requires a champion on the management team - a Management Representative. The Management Representative would usually be the security coordinator with responsibility for the day-to-day running of the ISMS.

As the title implies, the Management Representative is the link between the operating ISMS and the company Management through the Management Review function. The Management Representative will bring to the attention of Management persistent or recurring problems or those which cannot be actioned at any other level. These problems may be highlighted through normal quality control and assurance activities but will also include the results of internal audits.

The Management Representative is responsible for ensuring that the requirements of the organization in terms of policy, objectives and supporting processes, are implemented and maintained. Usually the security coordinator is also responsible for running the ISMS on a day-to-day basis. The role must carry the necessary authority to be able to fulfil these responsibilities. The security coordinator may hold other, but not conflicting, roles.

14.5.6.5. Auditors . . .

The security coordinator will normally be responsible for selecting, training and managing the internal auditors, scheduling internal audits, monitoring the implementation of the audit schedule and reporting to the Management Review Body. Like most activities this set can be delegated.

The number of auditors required will depend on the size of the company, the scope of the ISMS and the diversity of the functions carried out within the ISMS. For example, a manufacturing company of about 800, spread over 3 sites, could manage with a team of 24 internal auditors representing all major functions covered by the ISMS.

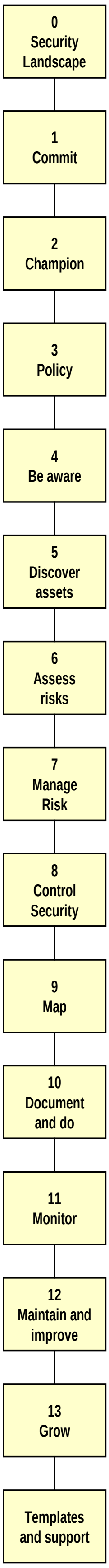
The auditors must be independent of the function or department being audited. This prevents (or at least minimises) conflicts of interest and company politics intruding into what should be seen as a constructive and helpful activity.

Auditing is about communication with emphasis on listening. After all, ‘auditor’ means ‘hearer’ or ‘listener’. The auditor must also be equipped to ask the right questions in order to get the information required. Good auditors have, or will develop, a very definite set of qualities such as those listed above. We will look at the qualities of auditors (and their auditees!) in more detail later.

Usually internal auditors will be selected from the functions which are covered by the scope of the ISMS. The idea is to provide a large enough pool of auditors to be able to carry out the audit schedule and still provide the necessary degree of independence. In general, internal auditors will continue with their primary role within the company. Auditing will be a second role and this has to be borne in mind by the security coordinator when scheduling audits.

The audit schedule – take a risk based approach but be thorough to take in all eventually:

- New tools installed
- New hardware
- New staff
- Changes in privileges



- Changes in roles
- Especially when higher access rights granted (is this part of the bullet above?
- Regular process checks
- On-going password checks
- Firewall event logging
- Software license checks
- Virus tool reports
- Vulnerability audits

A sample audit schedule could cover:

- First complete, and subsequently reviewed, statement of applicability
- Check of adequacy of the business continuity plan
- Security controls
- Use of new reporting logs
- New CRM Software Implementation
- Website compliance to DDA standards
- Business Continuity Plan
- Disposal of old records
- 'MOT' audits of laptops[80]
- Personnel record audit cycle
- Extension of security controls

14.5.6.6. How to carry out an audit: an overview

The audit is conducted against an objective reference base - the documented ISMS and/or a standard. It is conducted by auditors who are independent of the area they are auditing. This means, in practice, that there must be no conflict of interest, for example line-management control, for the auditor.

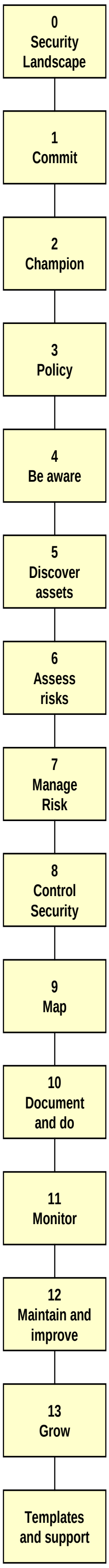
The objective reference base and the independence of the auditor help to ensure that company politics and personal prejudice do not influence what ought to be an unbiased assessment of practice.

The typical audit cycle will include:

- A preparation stage during which the auditor will carry out a reconnaissance or pre-audit of the function to be audited
- Deciding the scope of the audit
- Preparing a checklist of pertinent questions to be covered during the audit

The auditee, often the manager or supervisor of the function being audited, may receive a copy of the checklist prior to the audit.

The execution of the audit usually starts with an opening meeting, to clarify the scope of the audit and answer any questions that the auditee might have about the process. As everyone becomes familiar with the audit process this stage will become quite short. During the audit, any non-conformances will be noted and cross-referenced to either the documented ISMS or the standard. Any audit trails which lead out of the scope of the audit will be noted and picked up by other auditors during the appropriate audit. The execution of the audit closes with another meeting with the auditee to agree the non-conformances, perhaps discuss corrective action and decide dates for actions to be completed.



[80] Ensure remote users have not added anything else onto their system which could compromise the network integrity, altered settings that control security policies, or failed to load the relevant patches or antivirus updates.

Non-conformances, corrective action and dates for completion will form the audit report. The report should be prepared immediately the audit is completed within 24 hours.

The audit is not considered to be closed until all corrective actions have been completed and the auditor has confirmed that this is the case. This confirmation is the follow-up audit and will be confined to the corrective actions. In other words the follow-up audit is not a complete re-audit.

14.5.6.7. Audit results

The data provided by audits needs to be analysed to:

- Discover trends and confirm improvements
- Highlight difficulties in the application of processes or in particular activities or parts of a process
- Give an idea of the types of corrective action being carried out and how long corrective action takes to implement

The types and numbers of non-conformances may highlight the need for more training, either technical training or training in the use of the processes themselves.

The results of audits will also influence the scheduling of future audits.

Collating and analysing audit results is usually the responsibility of the security coordinator. Trends and highlighted problems, or problem areas, will form the basis of the report to the Management Review body.

14.5.6.8. Management Review function

The purpose of this body is to review, regularly, the performance and continued relevance of the ISMS. It is expected to respond to problems which cannot be solved at any other level within the ISMS for whatever reason.

The body will review measurement information from a number of sources in addition to the results from the internal audit system, including security incident reports. Again, the collation of this information is usually the responsibility of the security coordinator.

Without review and action at this level the ISMS may become irrelevant to the business, inflexible and bureaucratic.

14.5.6.9. Management Review agenda

If there is a single activity that can start the ball rolling towards an effective ISMS in your organisation it is getting security on to the management agenda. This goes right back to that initial buy-in from management that we referred to in stage one. Of course if we include that agenda there, it would have needed so much explanation that you would still be reading that section and this ISMS development method would lose its structure. So that vital injection of structure and compliance that you can make – and given that there will be some sort of quasi-regular management get together wherever you are – should comprise:

(1) Results of internal audits

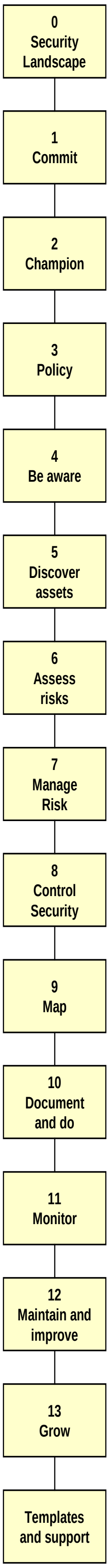
(2) Measurements and their interpretation from:

    (a) Corrective action or issues reports

    (b) Security incident reports

    (c) Statistics

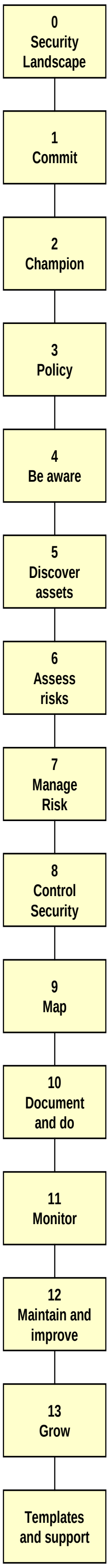
(3) Second/third party audit report/findings



- (4) Policy scope and objectives review
- (5) Security issues
    - (a) Risk management
        - (i) Containment of risk within acceptable levels
        - (ii) Reduction of overall risk
    - (b) Process performance
    - (c) Legal and regulatory issues
- (6) Actions for improvement
- (7) AOB
- (8) Conclusion

14.6. The role of the security expert

Your security expert should be active in your review process – possibly carrying out some of the internal audit checks for you. Also, your expert should review the outcomes of your checks to help you to get a feel for the severity of what you find so that commensurate actions may be delegated.



15. Stage 12 - Maintain the ISMS and Ensure Continuous Improvement

15.1. Purpose

Implementing ISMS will not ensure sudden improvement in the information assurance of your organisation. It provides an opportunity to monitor the security in an organised manner and ensure continuous improvement. Ensure that the continuous improvement actually takes place by defining measures (plan), running your business (do), reviewing those measures for – say - reduced risk, and increase or reduce security activity according to the results of the review (act).

The concept of environmental change is quite straightforward. There are two sources of change: the organisation, and the rest of the world.

Change in the organisation is easy to understand. New systems will be deployed; upgrades will be applied; new applications will be written; firewalls will be reconfigured. The systems will always be in a state of flux, and this is normal and usually considered an acceptable risk. It is certainly a better option than ‘freezing’ a system, which denies the possibility of patches enhancing the performance, security and functionality of the system, and also the possibility of meeting emerging business requirements.

Meanwhile the rest of the world is busy too. Two groups of people will be spending a great deal of time looking for security holes in applications and operating systems – security professionals, and skilled hackers. Every day, security advisories are published drawing attention to newly discovered problems; these discoveries – often theoretical – are quickly developed into workable exploits, and then the hacking community at large is able to start breaking into systems previously believed to be secure.

15.2. Audience

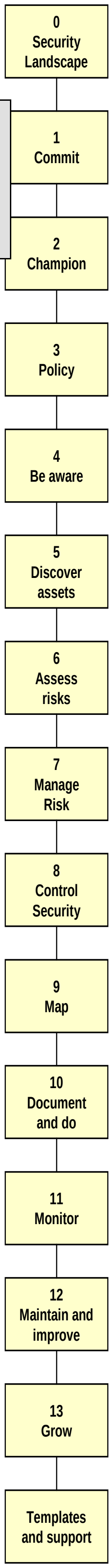
At the risk of sounding repetitive, this is something that involves all stakeholders in the organisation. It is important to have an organisational culture that shares information such as security incidents so that lessons can be learnt, corrective action taken and preventive action put in place without fear of blame.

The security coordination activity will be at the forefront monitoring the risks and threats faced by other organisations as reported in the many bulletins, alerts and newsletters to ensure that the policies of the ISMS and their implementation remains commensurate with the level of protection required.

15.3. Deliverables

Any part of the ISMS may be updated as a result of this on-going activity, especially:

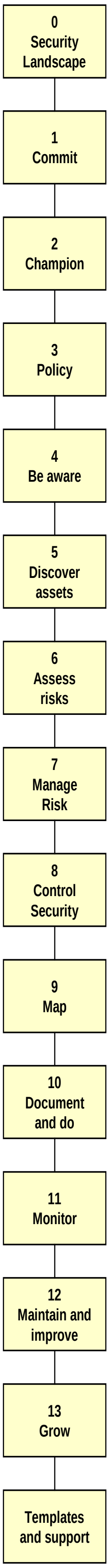
- ISMS processes and procedures
- ISMS scope[81]
- Operational processes
- Risk assessment report
- Risk treatment plan
- Security policy
- Statement of applicability



[81] This is especially likely to change when a new business stream is adopted or a current stream ended.

15.4. Successful techniques

15.4.1. Measurement



Two key attitudes to have here:

(1) Be proactive

(2) Measure

It is essential to know what you are improving and some objective measurement is essential. Look at two kinds of measure:

- **Direct improvements**: the ISMS is getting better at reducing risk, incidents are costing less to correct, more incidents are being prevented through early risk reporting and so on. You are improving the effectiveness of the ISMS.
- **Indirect improvements**: Your tools and methods that comprise part of your ISMS are improved either in themselves (say the deployment of automated heuristic analysis of firewall logs over manual scanning) or the way that the controls are being measured (for example better time recording of disaster recovery activity).

Use your management review (established in the previous stage) process to:

- Regularly review and decide the criteria for accepting risks and the acceptable levels of risk, based on the incidents that are realised and the results on internal audits of the ISMS
- Use the following as inputs to your management review:
  - The information security policy
  - Information security objectives
  - Internal audit results
  - Analyses of monitored events
  - Corrective and preventive actions
- Make sure that the recommended improvements are implemented and are having the expected effect

Identify opportunities for improvement from:

- New business requirements, particularly the interaction of business processes or business processes applied to new work. This is a constant test of the ability of your ISMS to be agile with integrity
- New threats that are identified by you, your staff, or the many sources of alert be they specialist bulletins or national news
- Internal, second and third-party audits

15.4.2. Change management

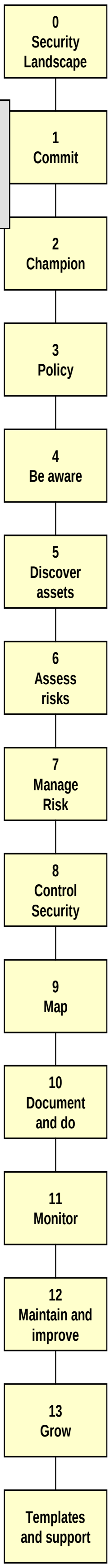
Improvements will mean some sort of change. Include your security champions in the review and approval of changes to ensure that there is adequate attention given to the impact of change. Like the ISMS, changes may best be tested out in one or more discrete areas of activity before they are rolled out across the organisation.

15.5. The role of the security expert

This is the stage where you should be able to handover your external view and opinion to the assessor or registrar of your ISMS (assuming that you decide to take that extra step of third-party scrutiny). This will maintain continuity and continue to provide that external view. You may find it worthwhile to have a handover period where your security expert is there to advocate your decisions to your assessor/registrar until you have the experience and relationship with the assessor/registrar to do this.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

16. Stage 13 - Extending the Scope of the Security Management System



16.1. Purpose

Businesses will change. In fact a complex business may implement an ISMS in phases by concentrating on certain areas or processes and then extending the scope until it is suitably comprehensive. The ISMS must manage change and integrate new scenarios and business activities into current practices or extend those practices as necessary.

16.2. Audience

The top management team of the organisation take responsibility for the ISMS in the same way that they take responsibility for the business. They must review the scope of the ISMS regularly to make sure that it reflects the business needs. Off course, starting or closing a business stream may have significant impact on the scope and so this may need to be addressed sooner than the regular management review session.

16.3. Deliverables

Extending the scope of the ISMS would affect one or more of the documentary items of the ISMS. In the table below, we've tried to show where the most changes are likely to be needed and why.

Security policy

The top level policy is unlikely to need changing but the detailed policies in your statement of controls are likely to be affected by changes in business, especially if it means something like changes in your supply chain or, say, allowing your staff mobile or wireless computing devices.

ISMS scope

This will change depending on how generic you make it – you may have a generic scope that refers to types of business or you may be more specific. The latter is more likely to change.

ISMS processes and procedures

These should be subject to constant review and updating according to circumstance. However, if you have achieved a process-based ISMS rather than a product or departmental-based ISMS, then the amount of change will not exceed your usual updating of your documentation.

Risk assessment report

This will change in advance of the change to scope because you will need to carry out a risk assessment to understand the impact the proposed extension to your scope will have.

Risk treatment plan

Difficulties thrown into relief by your risk assessment report will not damage the effectiveness of your ISMS if they are counterbalanced by the appropriate treatment for the risk. The updated or supplementary risk treatment plan will manage the risks taken on board.

Statement of applicability

As a result of your extension to the scope of the ISMS it is highly likely that you will be adopting new controls or extending the controls that you have in place. You must update your statement of applicability but do this as an internal audit so that you are, at the same time, verifying that the necessary security measures are in place as a result of the changes.

Business continuity plan

The risk assessment for your change of scope may identify new information assets that may need scrutiny or it may alter the priorities or contingency plans for business continuity. Your business continuity plan must follow suit.

Processes and procedures

These will be improved with practice – the rough edges of initial issues will be polished, processes will be streamlined and amalgamated to be simpler[82].

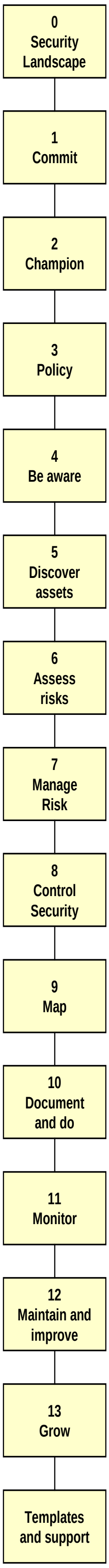
16.4. Successful techniques

As the table above suggests, the smooth transition from one scope to another and the integration of new measures into the ISMS can be achieved concentrating on the plan-do-check-act cycle of:

- Risk assessment
- Risk treatment
- Internal audit – updating the statement of applicability
- Updating and implementing the ISMS processes and procedures

16.5. The role of the security expert

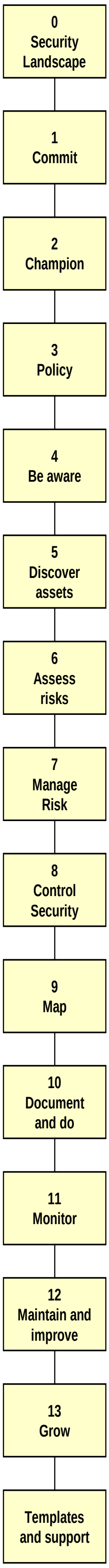
If you make major changes to your ISMS it will not be appropriate to compromise the independence of your assessor registrar to make lots of comment on your activities. You may wish to engage your security expert again at these times depending on the expertise that you develop during your time developing and maintaining the ISMS.



[82] In the event of extending an ISMS following mergers and acquisitions, be prepared to have multiple approaches to the same issues. If you seek the Eldorado of commonality too soon you are more likely to stop the acceptable practices without adequate controls to replace them.

17. To Certify – Or Not?

17.1. Third party assessment



The effort to define, implement and manage an ISMS is not insignificant (although it is described here in such a way as to be done as a necessary component of good corporate governance). As time goes on, the difficulty will be to maintain the initial impetus and to keep it fresh and up to date – one reason for defining ‘continuous improvement’ as a discrete phase of the method. One of the best carrots (not sticks) to encourage organisations to manage their systems is the framework of external assessment to benchmark ISMS against the ISO/IEC 27001 standard (or more accurately the management system that assesses risk and selects appropriate controls from the ISO/IEC 27002 ‘catalogue’). This is an expense but relatively small compared to the effort of information assurance for the organisation overall. Third party assessment is not really a consultative process but a good assessment body will get leave you with the benefits of having had a consultant in but with the confidence to be independent enough to implement their recommendations yourself. Select an accredited, third-party assessor or registrar who will:

- Act as a partner in the continuing development of your ISMS, taking the role of the ‘security expert’ you engaged originally for third-party advice
- Work with you on risk-based assessments so that they will be just as thorough yet concentrate their scrutiny where it is most likely to help
- Provide a certification service to show compliance with the standard
- Bring a regular external view of your ISMS to benchmark your continuous improvement
- Promote information assurance as a key objective for your organisation amongst the many other pressures that it faces

17.2. Sed quis custodiet ipsos custodes[83]?

Any organisation, in theory, can certify another as being compliant with ISO/IEC 27001. The challenge is to ensure that the certification carries authority. Fortunately the UK Accreditation Service (UKAS) exists to maintain a register of companies and organisations that it authorises to perform accreditations.

The businesses on this register will provide valuable assistance and advice in the development and implementation of an ISMS. They will have staff who will be able to provide guidance at every stage of the process, and who should be considered allies, not adversaries.

Such companies will employ qualified and registered auditors, and they will use a strictly defined methodology for assessing whether an ISMS is compliant with the standards. The organisation being assessed must provide the auditors with the required background information: documents showing the stages of development of the ISMS, the ISMS documentation itself, and justification of the various decisions taken along the way.

17.3. A helpful process

There are usually three steps to the assessment process. Make sure that they are working for you as a positive checking and reporting mechanism. Most assessment bodies will offer:

(1) **Stage 0**
A Preliminary assessment or gap analysis
Are you ready?
A voluntary visit that can make sure that your interpretation of the standard is up to scratch. It’s an opportunity for you to expose your organisation to the assessment body without the

[83] But who watches the watchmen

pressure of this being the ‘make or break’ assessment. It also helps in the awareness process if you publicise this stage because it often precedes the ‘real’ assessment by some months.

(2) **Stage 1**
Document review
Do you say you do enough?
The assessor will look to see that you have (at the appropriate stage of development):

- Security policy
- ISMS procedures
- Risk Treatment plan
- Records
- ISMS Scope
- Risk Assessment report
- Operational procedures
- Statement of Applicability (showing the excluded controls and the traceability to your risk assessment)

Make sure that you can explain your risk assessment methodology and how you identify your information assets. How you pick up threats, and vulnerabilities and the impact they may have. The assessor will look to see that you are being specific not generic. You will need to clearly show the acceptance of risk as you reach the acceptable level (understanding how that level is set) and the authorisation to work where that level is exceeded.

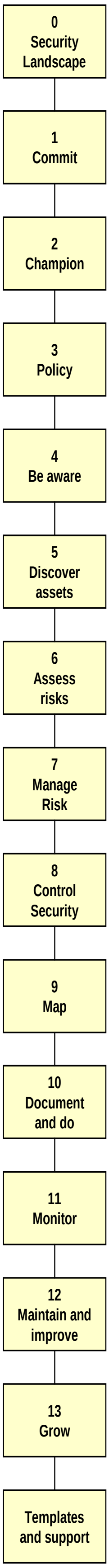
(3) **Stage 2**
An audit against the Statement of Applicability
Are you doing enough?
Assessors want confidence that the ISMS – with appropriate controls - is effectively implemented. Can you provide evidence of your information assurance activities? The assessor will look for:

- Plan-Do-Check-Act culture
- Resource management
- Internal Audit
- Corrective action
- Management responsibility
- Management review
- Continual improvement
- Preventive action

This is a positive assessment. The assessor will look for compliance. However, if incidences of non-compliance with the ISMS standard are found, they will be reported respectively as corresponding to:

· An observation	That should be considered as part of the continuous improvement programme
· A minor non-compliance	Something that needs to be dealt with adequately before the next surveillance visit
· A major non-compliance	A problem that prevents a certificate being granted

(4) An assessor who has seen enough evidence of an effective ISMS will recommend the organisation for approval. This recommendation undergoes a technical review by the assessors’ organisation and it is generally unusual for the certificate not to be granted at this stage as a result of the careful selection and training of assessors.



(5) The outcome of the assessors audit will end without a recommendation for approval should insufficient evidence of an effective ISMS be forthcoming. This will probably mean a follow-up audit after a period of 3 months to take corrective action. If this stretched to 6 months, the assessor will return and scrutinise your commitment to information security by reviewing the evidence of management taking responsibility for it. Should this follow-up period lapse to 12 months, the assessor will go through a complete re-assessment.

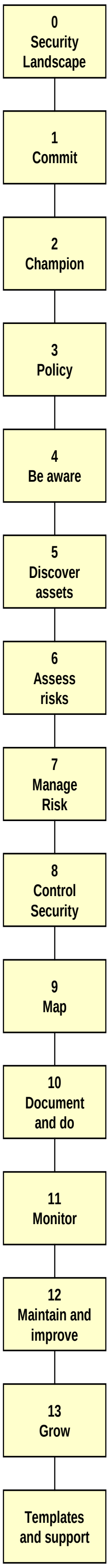
(6) Successful completion of stage 2 starts the surveillance cycle. Your certification lasts for 3 years, depending on maintaining a healthy ISMS during that period. To verify that, your assessor returns every six to nine months (depending on the size of organisation and the scope of your management system) to sample your business activities. Again, this sampling should be risk based. It is usually economic to consider any changes to approval at the time of a surveillance visit. Surveillance visits will typically look at how you've faired with regard to:

- Policy and objectives
- Management review
- Incident monitoring
- Objectives
- Corrective action
- Continual improvement
- Significant changes
- Internal audit
- Risk assessment and treatment
- Statement of applicability
- Preventive action
- Sample of controls

As with the original assessment, non-compliance are reviewed within 3 to 6 months, and a certificate can be withdrawn if corrective action is not taken.

(7) Before the end of the three years certification period, your assessor will plan your reassessment with you, keeping an eye on any change of activity that may affect the scope.

Note: Remember Stage 13. Make the most of your assessment fees by scheduling changes to the scope of your ISMS' approval to coincide with a regular assessment visit rather than creating additional administration of organising another visit.



18. Summary

The development and maintenance of an ISMS can be successfully implemented by planning and carrying out a structured set of activities based on these stages:

(1) Persuade top management of the need to act on security issues

(2) Appoint security champions to represent all activities

(3) Compose and agree your high level security policy

(4) Create security awareness: train and educate staff

(5) Identify and classify the assets

(6) Assess the risks to your information assets

(7) Plan how to reduce risk to an acceptable level

(8) Establish pragmatic security policies

(9) Map out where your security controls should be

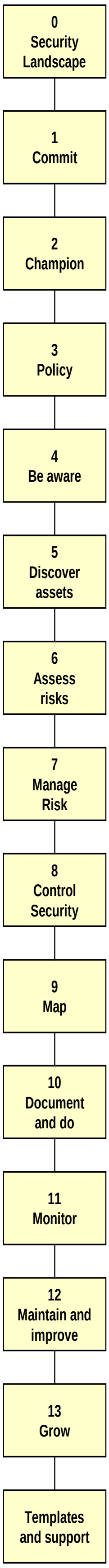
(10) Write and implement your system security plans, processes, and procedures

(11) Monitor and review the ISMS performance

(12) Maintain the ISMS and ensure continuous improvement

(13) Extending the scope of the security management system

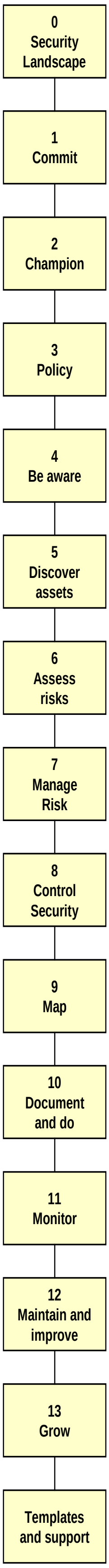
These stages may be discrete but they are likely to provide a set of milestones against which you can benchmark your information assurance activities whilst you integrate them with your organisation's current activities.



19. Conclusion

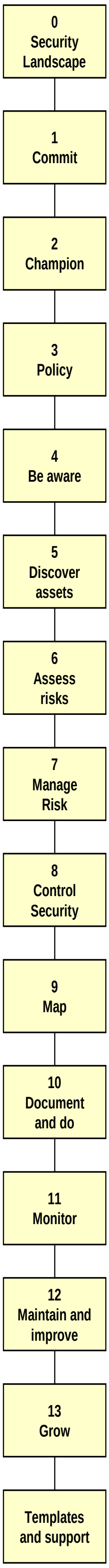
The strength of ISO/IEC 27001 and ISO/IEC 27002 is the realistic risk-based approach and the opportunity to take an informed and honest view of operational activities to determine what risks are acceptable and what measures must be taken for assurance of information across the enterprise.

It turns out that accepted wisdom has it that government and military activities require a ‘higher standard’ of information assurance that that provided by ISO/IEC 27001 and ISO/IEC 27002. This is not so. ISO/IEC 27001 is a framework and the controls of ISO/IEC 27002 adopted therein for any single organisation, or circumstance, are those based on the respective risk assessment. It is just that for these apparently more stringent requirements of the government and the military, the government and the military have carried out the risk assessment and identified the controls commensurate with the results. Organisations that have adopted a standards-based framework for their information assurance find that they have the structure to adopt the new controls of future business requirements.



Appendix A. Glossary

BS	British standard
COTS	Commercial off-the-shelf software
CRM	Customer relationship management
ICT	Information and communications technology
ISMS	Information security management system
ISO	International standards organisation
PKI	Public key infrastructure
SLA	Service level agreement
VPN	Virtual private network



Appendix B. Statement of Applicability Template

The following pages may be copied to create your own statement of applicability

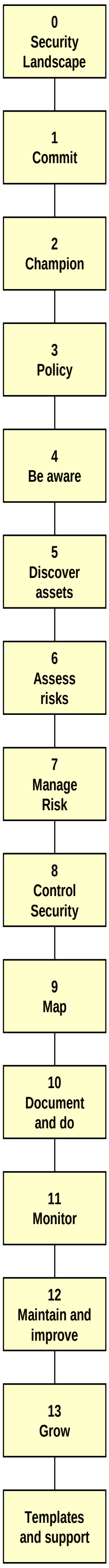
Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
4 RISK ASSESSMENT AND TREATMENT					
4.1 ASSESSING SECURITY RISKS					
4.2 TREATING SECURITY RISKS					
5 SECURITY POLICY					
5.1 INFORMATION SECURITY POLICY					
5.1.1 Information security policy document					
5.1.2 Review of the information security policy					
6 ORGANISING INFORMATION SECURITY					
6.1 INTERNAL ORGANISATION					
6.1.1 Management commitment to information security					
6.1.2 Information security co-ordination					
6.1.3 Allocation of information security responsibilities					
6.1.4 Approval process for information processing facilities					
6.1.5 Confidentiality agreements					
6.1.6 Contact with authorities					
6.1.7 Contact with special interest groups					
6.1.8 Independent review of information security					
6.2 EXTERNAL PARTIES					
6.2.1 Identification of risks related to external parties					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
6.2.2 Addressing security when dealing with customers					
6.2.3 Addressing security in third party agreements					
7 ASSET MANAGEMENT					
7.1 RESPONSIBILITY FOR ASSETS					
7.1.1 Inventory of assets					
7.1.2 Ownership of assets					
7.1.3 Acceptable use of assets					
7.2 INFORMATION CLASSIFICATION					
7.2.1 Classification guidelines					
7.2.2 Information labelling and handling					
8 HUMAN RESOURCES SECURITY					
8.1 PRIOR TO EMPLOYMENT					
8.1.1 Roles and responsibilities					
8.1.2 Screening					
8.1.3 Terms and conditions of employment					
8.2 DURING EMPLOYMENT					
8.2.1 Management responsibilities					
8.2.2 Information security awareness, education and training					
8.2.3 Disciplinary process					
8.3 TERMINATION OR CHANGE OF EMPLOYMENT					
8.3.1 Termination responsibilities					
8.3.2 Return of assets					
8.3.3 Removal of access rights					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
9 PHYSICAL AND ENVIRONMENTAL SECURITY					
9.1 SECURE AREAS					
9.1.1 Physical security perimeter					
9.1.2 Physical entry controls					
9.1.3 Securing offices, rooms and facilities					
9.1.4 Protecting against external and environmental threats					
9.1.5 Working in secure areas					
9.1.6 Public access, delivery and loading areas					
9.2 EQUIPMENT SECURITY					
9.2.1 Equipment sitting and protection					
9.2.2 Supporting utilities					
9.2.3 Cabling security					
9.2.4 Equipment maintenance					
9.2.5 Security of equipment off-premises					
9.2.6 Secure disposal or re-use of equipment					
9.2.7 Removal of property					
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT					
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES					
10.1.1 Documented operating procedures					
10.1.2 Change management					
10.1.3 Segregation of duties					
10.1.4 Separation of development, test and operational facilities					
10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT					
10.2.1 Service delivery					



Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
10.2.2 Monitoring and review of third party services					
10.2.3 Managing changes to third party services					
10.3 SYSTEM PLANNING AND ACCEPTANCE					
10.3.1 Capacity management					
10.3.2 System acceptance					
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE					
10.4.1 Controls against malicious code					
10.4.2 Controls against mobile code					
10.5 BACK-UP					
10.5.1 Information back-up					
10.6 NETWORK SECURITY MANAGEMENT					
710.6.1 Network controls					
10.6.2 Security of network services					
10.7 MEDIA HANDLING					
10.7.1 Management of removable computer media					
10.7.2 Disposal of media					
10.7.3 Information handling procedures					
10.7.4 Security of system documentation					
10.8 EXCHANGES OF INFORMATION					
10.8.1 Information exchange policies and procedures					
10.8.2 Exchange agreements					
10.8.3 Physical media in transit					
10.8.4 Electronic messaging					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
10.8.5 Business information systems					
10.9 ELECTRONIC COMMERCE SERVICES					
10.9.1 Electronic commerce					
10.9.2 On-line transactions					
10.9.3 Publicly available information					
10.10 MONITORING					
10.10.1 Audit logging					
10.10.2 Monitoring system use					
10.10.3 Protection of log information					
10.10.4 Administrator and operator logs					
10.10.5 Fault logging					
10.10.6 Clock synchronisation					
11 ACCESS CONTROL					
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL					
11.1.1 Access control policy					
11.2 USER ACCESS MANAGEMENT					
11.2.1 User registration					
11.2.2 Privilege management					
11.2.3 User password management					
11.2.4 Review of user access rights					
11.3 USER RESPONSIBILITIES					
11.3.1 Password use					
11.3.2 Unattended user equipment					
11.3.3 Clear desk and clear screen policy					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
11.4 NETWORK ACCESS CONTROL					
11.4.1 Policy on use of network services					
11.4.2 User authentication for external connections					
11.4.3 Equipment identification in the network					
11.4.4 Remote diagnostic and configuration port protection					
11.4.5 Segregation in networks					
11.4.6 Network connection control					
11.4.7 Network routing control					
11.5 OPERATING SYSTEM ACCESS CONTROL					
11.5.1 Secure log-on procedures					
11.5.2 User identification and authentication					
11.5.3 Password management system					
11.5.4 Use of system utilities					
11.5.5 Session time-out					
11.5.6 Limitation of connection time					
11.6 APPLICATION AND INFORMATION ACCESS CONTROL					
11.6.1 Information access restriction					
11.6.2 Sensitive system isolation					
11.7 MOBILE COMPUTING AND TELEWORKING					
11.7.1 Mobile computing and communications					
11.7.2 Teleworking					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

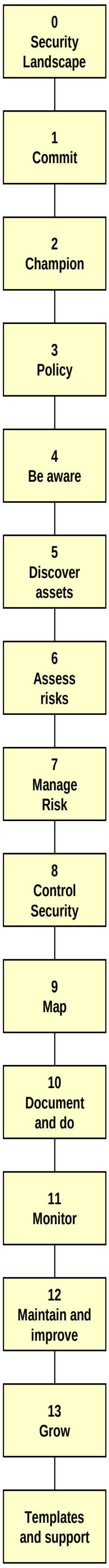
Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE					
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS					
12.1.1 Security requirements analysis and specification					
12.2 CORRECT PROCESSING IN APPLICATIONS					
12.2.1 Input data validation					
12.2.2 Control of internal processing					
12.2.3 Message integrity					
12.2.4 Output data validation					
12.3 CRYPTOGRAPHIC CONTROLS					
12.3.1 Policy on the use of cryptographic controls					
12.3.2 Key management					
12.4 SECURITY OF SYSTEM FILES					
12.4.1 Control of operational software					
12.4.2 Protection of system test data					
12.4.3 Access control to program source code					
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES					
12.5.1 Change control procedures					
12.5.2 Technical review of applications after operating system changes					
12.5.3 Restrictions on changes to software packages					
12.5.4 Information leakage					
12.5.5 Outsourced software development					
12.6 VULNERABILITY MANAGEMENT					
12.6.1 Control of vulnerabilities					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

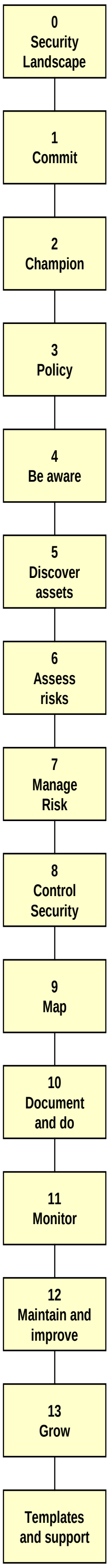
Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
13 INFORMATION SECURITY INCIDENT MANAGEMENT					
13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES					
13.1.1 Reporting information security events					
13.1.2 Reporting security weaknesses					
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS					
13.2.1 Responsibilities and procedures					
13.2.2 Learning from information security incidents					
13.2.3 Collection of evidence					
14 BUSINESS CONTINUITY MANAGEMENT					
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT					
14.1.1 Including information security in the business continuity management process					
14.1.2 Business continuity and risk assessment					
14.1.3 Developing and implementing continuity plans including information security					
14.1.4 Business continuity planning framework					
14.1.5 Testing, maintaining and re-assessing business continuity plans					
15 COMPLIANCE					
15.1 COMPLIANCE WITH LEGAL REQUIREMENTS					
15.1.1 Identification of applicable legislation					
15.1.2 Intellectual property rights (IPR)					
15.1.3 Safeguarding of organisational records					

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Control	Implemented where	Justification if not applied	Tools and methods used	Notes and comments	Action; by whom; by when
15.1.4 Data protection and privacy of personal information					
15.1.5 Prevention of misuse of information processing facilities					
15.1.6 Regulation of cryptographic controls					
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS					
15.2.1 Compliance with security policy and standards					
15.2.2 Technical compliance checking					
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS					
15.3.1 Information systems audit controls					
15.3.2 Protection of information systems audit tools					



Appendix C. Bibliography and further reading



ALARM (February 2001). *A key to success - a guide to understanding and managing risk*.

Alexander, I.F. (2007). *A Taxonomy of Stakeholders: Human Roles in System Development*, Issues and Trends in Technology and Human Interaction, Editor(s): Bernd, Carsten, Stahl (De Montfort University, UK) IRM Press. 25-71 pp.

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems,* 2nd Edition, Wiley Publishing Inc.

Argyris, C.; and Schön, D. (1974) *Theory in practice: Increasing professional effectiveness*, San Francisco: Jossey-Bass.

Armstrong, J., Rhys-Jones, M., and Dresner, D. (2004). *Managing Risk: Technology and Communications, Lexis Nexis*.

Ashby, W. R., (1957). *An introduction to Cybernetics*, Second impression, London. Chapman and Hall Limited.

Australian Agency for International Development (2000). *AusGUIDElines, 5. Managing risk*, The Australian Government’s Overseas Aid Program.

Backhouse, J., Hsu, C.W., and Silva, L. (2006). *Circuits of power in creating de jure standards: shaping an international information systems security standard*, MIS Quarterly Vol. 30 Special Issue on Standard Making, pp. 413-438.

Banfield, E. (2001). *Dredge first hedge later*, Risk Professional 1/2001, S. 40-43.

Barker, W.C. (2004), Special Publication 800-60, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*, National Institute for Standards and Technology (NIST).

Baskerville, R. L. and Wood-Harper, A. T., (1996). *A critical perspective on action research as a method for information systems research*, Journal of Information Technology, Volume 11, Issue 3, pages 235 – 246

Beer, S. (1993). *World in Torment: A Time Whose Idea Must Come*, Presidential Address to the Triennial Congress of the World Organization of Systems and Cybernetics, New Delhi, India, January 1993. Kybernetes, Vol. 22 No. 6, 1993, pp. 15-43

Bernstein, P. L. (1998) *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons

Bevan, N., and Macleod, M. (1994) *Usability measurement in context*, Behaviour and Information Technology, 13, 132-145

BIP 0051:2004 ITIL. *Service support*, British Standards Institution

British Computer Society/Royal Academy of Engineering (2004). *The Challenges of Complex IT Projects*, Royal Academy of Engineering

British Standards Institution (2000), ISO/IEC 17799 (BS 7799) Part 1:2000 *Information security management: Code of practice for information security management.*

British Standards Institution, (2001). *The TickIT Guide: Using ISO 9001:2000 for Software Quality Management System Construction, Certification and Continual Improvement*.

British Standards Institution, 1998, BS 7925-1 *Vocabulary of terms in software testing*.

British Standards Institution, BS 25777:2008, *Information and communications technology continuity management. Code of practice*.

British Standards Institution, BS 25999-1:2006, *Business continuity management – Part 1: Code of practice*.

British Standards Institution, BS 25999-2:2007 *Business continuity management – Part 2: Specification*.

British Standards Institution, BS 6079-3:2000 *Project management Part 3: Guide to the management of business related project risk*.

British Standards Institution, BS 7799-2:2002, *Information security management systems – specification with guidance for use*.

British Standards Institution, BS EN 61014:2003 *Programmes for reliability growth*.

British Standards Institution, BS IEC 62198:2001 *Project risk management — Application guidelines*.

British Standards Institution, BS ISO 8807:1989 *Information processing systems. Open systems interconnection. LOTOS. A formal description technique based on the temporal ordering of observational behaviour*.

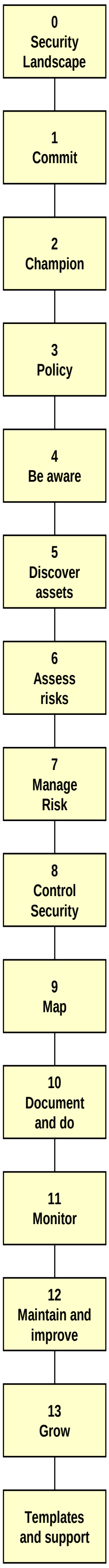
British Standards Institution, BS ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*.

British Standards Institution, BS ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice*.

British Standards Institution, BS ISO/IEC 27001:2005 BS 7799-2:2005 *Information technology — Security techniques — Information security management systems — Requirements.*

British Standards Institution, BS ISO/IEC 27002:2005 BS 7799-1:2005 *Information technology - Security techniques - Code of practice for information security management*, (Previously ISO/IEC 17799)

British Standards Institution, BS ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management measurements*.



British Standards Institution, BS ISO/IEC TR 15846:1998 *Information technology. Software life cycle processes. Configuration management*.

British Standards Institution, BS7858:2006 *Security Screening of Individuals in a Security Environment*.

British Standards Institution, PD 6668: 2001, *Managing Risk for Corporate Governance*.

British Standards Institution, PD CR 13694:1999, *Health informatics. Safety and security related software quality standards for healthcare* (SSQS).

British Standards Institution. BS 0:1997, *A standard for standards*.

Bryant, P. C., Davis, C. A., Hancock, J. I, and Vardaman, J. M. (2010), *When Rule Makers Become Rule Breakers: Employee Level Outcomes of Managerial Pro-Social Rule Breaking*, Employee Responsibilities and Rights Journal 22:101-112.

Bundesamt für Sicherheit in der Informationstechnik (2001). *IT Baseline Protection Manual*

Cabinet Office (2002). *Security: e-Government Strategy Framework Policy and Guidelines* Version 4.0, September 2002

Cabinet Office (2004). Central Sponsor for Information Assurance, *Protecting our information systems*, 262949/0604/D40.

Cabinet Office (2005). e-Government Unit, *e-Government Interoperability Framework* Version 6.1, Cabinet Office, 2005.

Cabinet Office (2005). *Transformational Government: Enabled by Technology*.

Cabinet Office (2008). *Security Policy Framework*

Cabinet Office e-Government Unit (2004). *e-Government Interoperability Framework, Technical Standards Catalogue*, version 6.1, 17 September 2004.

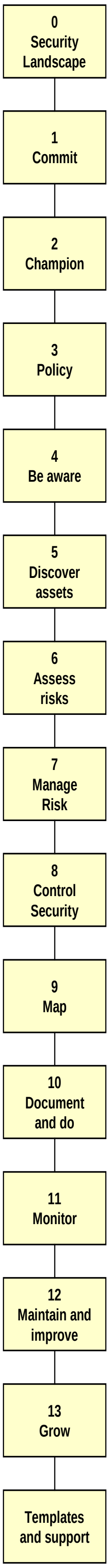
Cadbury Committee (1992). *Report of the Committee on the Financial Aspects of Corporate Governance*

Cappelli, D. M.,(2006). *Pay Attention! What are Your Employees Doing?* (Presentation).

Cappelli, D., Moore, A., Trzeciak, R. (2005). *Management and Education of the Risk of Insider Threat* (MERIT): System Dynamics Modeling of Computer System Sabotage, Carnegie Mellon CyLab.

Cappelli, D.M, Carnegie Mellon University, Keeney M. - United States Secret Service. (2004). *Insider Threat: Real Data on a Real Problem* (Presentation)

Cappelli, D.M, Moore, A., Trzeciak, R., Shimeall, T.J., (2009) Common Sense Guide to Prevention and Detection of Insider, Threats 3rd Edition – Version 3.1, CERT, Software Engineering Institute, Carnegie Mellon University.



Cappelli, D.M, Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E. A., Willke, B.J. (2006). *Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage*, CERT3 Program, Software Engineering Institute and CyLab at Carnegie Mellon University.

Carr, M.J., Konda, S.L., et al. (2003). *Taxonomy-Based Risk Identification*, Software Engineering Institute.

Cavanagh, M. C. (1997). *Ethics and Information Systems*, The National Computing Centre Guidelines for IT Management 224.

Cawthron, E. R. and Rowell, J. A.(1978). *Epistemology and Science Education, Studies in Science Education*, 5: 1, 31 – 59.

CESG ,(2005). HMG Infosec Standard No. 2 *Risk management and accreditation of information systems*, as published by NISCC, Issue 1.0, August 2005.

CESG, HMG (2009). HMG IA Standard No.6 - *Protecting Personal Data and Managing Information Risk* (originally known as the Minimum Mandatory Requirements).

CESG, HMG (2009). IA Standard No. 1, *Technical Risk Assessment*, Issue No: 3.51.

Checkland P. (1985). *From optimizing to learning: a development of systems thinking for the 1990s*, Journal of the Operational Research Society, 36 (9), 757 – 767.

Checkland P., and Holwell, S. (1998). *Information Systems and Information Systems: Making sense of the field*, Wiley,

Checkland, P. (1981). *Systems Thinking, Systems Practice*. John Wiley & Sons.

Cohen, F. (1997). *Information System Attacks: A Preliminary Classification Scheme*, Computers and Security, 16, 29-46.

Coles, R. and Hodgkinson, G. P. (2008). *A Psychometric Study of Information Technology Risks in the Workplace*, Risk Analysis, Vol. 28, No. 1.

Coles-Kemp. E., (2008). *The Anatomy of an Information Security Management System*, A thesis submitted for the degree of Doctor of Philosophy, Department of Computer Science King's College London, University of London

Crosby, P. (1979). *Quality is free: The Art of Making Quality Certain*, McGraw Hill.

Cusumano, M. A., Mylonadis, Y., and Rosenbloom, R. S. (1992). *Strategic Maneuvering and Mass-Market Dynamics: The Triumph of VHS over Beta*, The Business History Review, Vol. 66, No. 1, High-Technology Industries (Spring,), pp. 51-94.

Deming, W.E., (1950) *Elementary Principles of the Statistical Control of Quality*, Union of Japanese Scientists and Engineers (JUSE)

Deming, W.E., (1986) *Out of the Crisis*, MIT Center for Advanced Engineering Study

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Defense Contract Management Command (1999), *PROCAS; Online Information Center Summary Document* November 1999, Department of Defense

Department for Environment, Food and Rural Affairs DEFRAS (2002)

Department of Trade and Industry (2005). DTI Economics Paper No. 12, *The Empirical Economics of Standards*, June 2005

Dourado, P. (2007) cited in '*The Little Book of Leadership*', The Leadership Hub.

Dresner, D.G., (1992). Usability Now!, *Usability Evaluation Within an ISO 9001 Quality System*.

Dresner, D.G., (1996). *Usability: Practical Hints and Tips for Applying Cognitive Psychology to User Interfaces*, The National Computing Centre Guidelines for IT Management 208.

Dresner, D.G., (2005) *Using standards to mitigate risk in information systems*, A Report to Support the Transfer of Research from MPhil to PhD, Submitted after two years of part-time research for the degree of MPhil.

Dresner, D.G., and Wood, J.R.G. (2007). *Operational risk: acceptability criteria*, The Third International Symposium on Information Assurance and Security (IAS 2007), IEEE CS Press.

Dresner, D.G., Wood, J.R.G., *CatalysIS: Are you, or have you ever been, a vulnerability?* Report of a feasibility study into the detection of human vulnerabilities in information systems for The Technology Strategy Board, 2007.

European Network and Information Security Agency, ENISA (2006). *Inventory of risk assessment and risk management methods*, ENISA ad hoc working group on risk assessment and risk management

Federal Reserve Bank of San Francisco (2002). *Economic Letter, Number 2002-02*, January 25, 2002

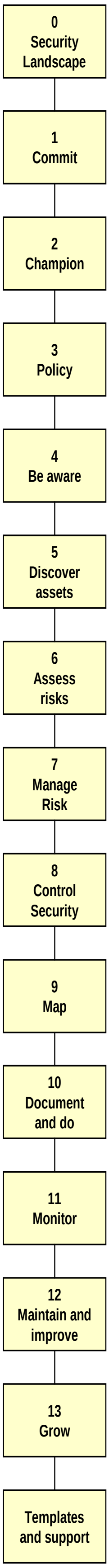
Financial Services Authority (2003). *The firm risk assessment framework*.

Flechais, I., Sasse, M.A., Hailes, S.M.V., (2003) Bringing security home: a process for developing secure and usable system\s, NSPW '03 Proceedings of the 2003 workshop on New security paradigms, ACM

Flechais, I., Riegelsberger, J., Sasse, A. M., (2005). *Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems*, New Security Paradigms Workshop '05, ACM.

Furnell, S.M., and Phyo, A.H., (2003). *Considering the problem of insider IT misuse*, Network Research Group, University of Plymouth.

Garud. R., and Kumaraswamy, A. (2005). *Vicious and virtuous circles in the management of knowledge: the case of infosys technologies*, MIS Quarterly Vol. 29 No. 1, pp. 9-33/March 2005.



Gotterbarn, D., and Rogerson, S., (2005). *Responsible risk analysis for software development: creating the software development impact statement*, CAIS.

Grafton, W., Bytheway, A., and Edwards, C., (1997). *Understanding user perceptions of information systems success*, The Journal of Strategic Information Systems, Volume 6, Issue 1, Pages 35-68.

Hayden, L., (2010) *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data: A Practical Framework for Measuring Security and Protecting Data*, McGraw-Hill Osborne

Harris, R., (2002). *Emerging Practices in Operational Risk Management, Federal Reserve Bank of Chicago*.

Hedlund, G. (1994). *A model of knowledge management and the N-Form Corporation*, Strategic Management Journal.

Heisenberg, W. (1927) *Ueber den anschaulichen Inhalt der quantentheoretischen Kinematik and Mechanik* Zeitschrift für Physik 43 172-198 (cited in the Stanford Encyclopedia of Philosophy, (http://plato.stanford.edu/entries/qt-uncertainty/)

Herzog, P., (2004). *Calculating Risk Assessment Values*, Institute for Security and Open Methodologies (ISECOM).

Higgs, D., *Review of the role and effectiveness of non-executive directors*. (2002).

Hillson D., and Murray-Webster, R., (2007).*Understanding and Managing Risk Attitude* (2nd edition), Gower Publishing.

House of Lords (2007). *Fifth Report of the House of Lords Science and Technology Select Committee* (10 August 2007), HL 165-II, p396 – 403.

Humphrey, C., and Scapens, R. W. (1996) *Rhetoric and case study research: response to Joni Young and Alistair Preston and to Sue Llewellyn*, Accounting, Auditing & Accountability Journal, Vol. 9 Iss: 4, pp.119 – 122

IEEE Computer Society (2004). *Guide to the Software Engineering Body of Knowledge* (SWEBOK).

IEEE Std 16085 (2003). *IEEE Standard for Software Life Cycle Processes—Risk Management*, (Previously IEEE Std. 1540-2001 and now ISO/IEC 16085:2006).

IEEE, (2004).*The Software Engineering Body of Knowledge*

Information Security Forum (2007). *The Standard of Good Practice for Information Security*.

International Standards Organisation, PD ISO/IEC Guide 73:2002, *Risk Management – Vocabulary – Guidelines for use in standards*.

International Standards Organisation. ISO/IEC 9126-1:2001 *Software engineering – Product quality – Part 1: Quality model*.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

International Standards Organisation. ISO/IEC 12207:1995 *Information technology — Software life cycle processes*, International Standards Organisation

International Standards Organisation. ISO/IEC 15288:2002 *Information Technology – Life Cycle Management – System Life Cycle Processes*, International Standards Organisation

International Standards Organisation, ISO/IEC TR 15504:1999 *Information technology - Software process assessment*.

International Standards Organisation, PD ISO/IEC TR 18044:2004 *Information technology — Security techniques — Information security incident management*.

ISO/IEC 25030:2007 *Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Quality requirements*.

International Standards Organisation. ISO/IEC 38500:2008 *Corporate governance of information technology*.

James, H.L., (1996). *Managing Information Systems Security: a Soft Approach*, IEEE.

Jiantao, P., (1999). *Dependable Embedded Systems, Software Reliability*, Carnegie Mellon University.

Joch, A., (December 1995). *Nine ways to make your code more reliable***,** Byte.

Kaplan, Robert S., and David Norton, (1992). *The Balanced Scorecard: Measures that Drive Performance*, Harvard Business Review 70, no. 1 (January-February 1992): 71-79.

Kaplan, B. and Maxwell, J.A., (1994) *Qualitative Research Methods for Evaluating Computer Information Systems*, in Evaluating Health Care Information Systems: Methods and Applications, J.G. Anderson, C.E. Aydin and S.J. Jay (eds.), Sage, Thousand Oaks, CA, 1994, pp. 45-68.

Khalil,O., Claudio, A., and Seliem, A.,(2006) *Knowledge management: the case of the Acushnet Company*, SAM Advanced Management Journal.

Kontio, J.,(1998). *The Riskit Method for Software Risk Management*, version 1.00, University of Maryland

Kuntz, T., (1998). *The Titanic Disaster Hearings, Pocket*

Lacey, D., (2008). *Talking about a revolution*, Infosecurity, Elsevier, October 2008

Lacey, D., James, B. E., (2010). *Review of Availability of Advice on Security for Small/Medium Sized Organisations, Information Commissioner's Office*

Leveson, N., and Turner, C.S., (1993). *An Investigation of the Therac-25 Accidents* – Part V, IEEE Computer, Vol. 26, No. 7, July 1993, pp. 18-41

Logica, (1987). *Quality Management Standards for Software*

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Lopez, J. A., (2003). *Overview of the Basel Committee's Second Working Paper on Securitization*, Economic Research Department, Federal Reserve Bank of San Francisco, 2003

Magklaras, G.B., and Furnell S.M., (2002). *Insider Threat Prediction Tool: Evaluating the probability of IT misuse*, Computers and Security Vol 21, No 1, pp62-73.

Myers, M.D., (1997) *Qualitative Research in Information Systems*, MISQ Discovery on May 20, 1997 (citing Kaplan and Maxwell 1994).

Morton, W., (2002). *Managing Risk: A Practical Guide*, National Computing Centre Guidelines for IT Management 265, 2002.

National Audit Office*, New IT systems for Magistrates' Courts: the Libra project*, Report by the Comptroller and Auditor General, HC 327 Session 2002-2003: 29 January 2003.

National Computing Centre, The, (1989). *The Starts Purchasers Handbook*.

National Computing Centre, The, (2000). *A Guide to Reviews from Desk Checks to Inspections.*

National Computing Centre, The, (2003). *Survey: Risk Management in IT*.

National Computing Centre, The, (2004). *Information Security Policy and Practice*.

National Computing Centre, The, (2004). *The National Computing Centre Guidelines for IT Management 289: Protect and Survive - Defending against application hacking*.

National Computing Centre, The, (2005). *An analysis of surveys for the Small Business Service of the Department of Trade and Industry*.

National Hi-tech Crime Unit, (2004). *Hi-Tech Crime: The Impact on UK Business*.

NISCC, (2002). Technical Note 04/02 *The Security of 802.11 Wireless Networks*.

NISCC, (2005). Policy and Best Practice 00759 NISCC Best Practice Guide. *Protecting Data Centres*.

Nonaka, I., and Hirotaka T., (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, New York, NY: Oxford University Press.

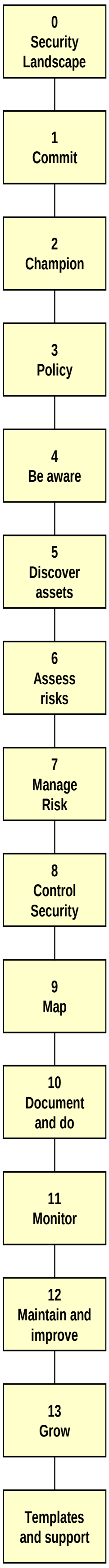
Nonaka, I., Toyama, R., and Konno, N., (2000). *SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation*.

Office of Government Commerce (2003), *Successful Delivery Toolkit*, Version 4.02, October, OGC.

Organisation for Economic Cooperation and Development, (2002). *Guidelines for the Security of Information Systems and Networks,* OECD.

Orlikowski, W. J. and Baroudi, J. J., (1991) *Studying Information Technology in Organizations: Research Approaches and Assumptions*, Information Systems Research, Vol. 2, No. 1, March 1991, pp. 1-28

Parliamentary Office of Science and Technology. (2003). *Government IT Projects* (POST).



Phyo, A.H., Furnell, S.M., (2003). *Data gathering for insider misuse monitoring, Network Research Group, University of Plymouth*.

Phyo, A.H., Furnell, S.M., (2004). *A detection-oriented classification of insider IT misuse, Network Research Group*, University of Plymouth.

Pickford, J. (Ed.), (2001). *Mastering Risk Volume 1: Concepts*, Financial Times,

Popper, K., (1963). *Conjectures and Refutations*, London: Routledge and Keagan Paul, pp. 33-39

Price Waterhouse (1988). *Software Quality Standards: the Costs and Benefits*

Price Waterhouse Coopers, (2004). *Information Security Breaches Survey 2004*, Department of Trade and Industry.

Price Waterhouse Coopers, (2006). *Information Security Breaches Survey 2006*, Department of Trade and Industry.

Price Waterhouse Coopers, *Information Security Breaches Survey, 2010*, Department for Business Innovation and Skill, 2010.

Price Waterhouse Coopers. (2010). *Information Security Breaches Survey 2010*, Department of Trade and Industry.

Professor Anthony Giddens, Reith Lectures, (1999).

http://news.bbc.co.uk/hi/english/static/events/reith_99/week2/week2.htm.

Randazzo, M.R., Keeney, M., Eileen Kowalski, E. (National Threat Assessment Center, United States Secret Service) Cappelli, D.M., Moore, A., (CERT® Coordination Center, Software Engineering Institute), (2005). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*.

Ranum. M., (2005). *The six dumbest ideas in computer security*, Information Security Bulletin, Volume 10, 285 – 290.

Riegelsberger, J., Sasse, M.A., McCarthy, J.D., (2005) *The mechanics of trust: A framework for research and design*, International Journal of Human-Computer Studies, Volume 62, Issue 3, Pages 381-422

Sasse, M.A., (2003) *Computer security: Anatomy of a usability disaster, and a plan for recovery*, CHI 2003, Workshop on HCI and Security Systems, ACM Press.

Sasse, M.A., Brostoff, S., and Weirich, D. (2002). *Transforming the 'weakest link' — a human-computer interaction approach to usable and effective security.* In R. Temple & J. Regnault (Eds.), Internet and wireless security (pp. 243-258). London: IEE.

Schein, E. H. (1976) *The Clinical Perspective in Fieldwork*, Sage University Papers Series on Qualitative Research Methods, Vol. 5, Thousand Oaks, CA, Sage.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Schultze, U., and Stabell, C., (2004) *Knowing what you don’t know?* Discourses and contradictions in Knowledge Management Research, Journal of Management Studies.

Seddon, J., (1998) *The Case Against ISO 9001*, ISO 9000 NEWS 4/1998, International Standards Organisation.

Shaw, E.D., Ruby, K.G., and. Post, J. M., (1998). *The Insider Threat To Information Systems, Security*, Awareness Bulletin No. 2-98, Department of Defense Security Institute.

Standish Group, (2003). *The CHAOS Report*

Stewart, T. A., (1997). *Intellectual Capital: The new wealth of organizations*,, Nicholas Brealey.

Stoneburner, G., Goguen, A., and Feringa, A., (2002). (NIST) Special Publication 800-30 *Risk Management Guide for Information Technology Systems, National Institute for Standards and Technology*

Swann, G. M. P., (2000). *The Economics of Standardization*. Department of Trade and Industry

Tanenbaum, A. S., (1980). *Computer Networks*, Prentice-Hall, Inc.

The Local eGovernment Standards Body, (2005). *Prospectus for operating an e-standards service*

Thomas, M., (1997) *Unsafe Standardization*, Computer, November. 1997, pp. 109–111.

Toynbee, A., (1949). *The Prospects of Western Civilization*, New York, Columbia University Press, by arrangement with Oxford University Press

Tuglular, T., (2000). *A Preliminary Structural Approach to Insider Computer Misuse Incidents*, EICAR Best Paper Proceedings.

Turnbull, N., (1999). *Internal Control: Guidance for Directors on the Combined Code,* Institute of Chartered Accountants in England and Wales, 1999

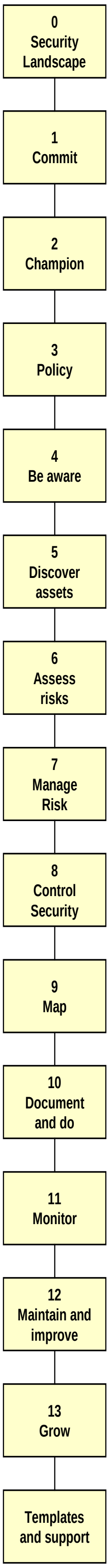
Turner, K., (2002). *Safety-Critical Systems: An Approach for Radiotherapy Equipment*, Department of Computing Science and Mathematics, University of Stirling.

US Office of the Under Secretary of Defense (2004). (Acquisition, Technology and Logistics) / Defense Systems.

Vara, V., (2007). Ten Things Your IT Department Won't Tell You, The Wall Street Journal, 30 July 2007

W3C, (2003). *World Wide Web Consortium Process Document*, World Wide Web Consortium 18 June 2003

William Knight, (2005). *Don’t let standards threaten innovation*, Computing, 10 February 2005



Appendix D. Risk Treatment Plan Template

This comes in two essential parts:

- The list of assets and their ranked values

Information Assets (for example: hardware, software, databases, comms. Lines)		Owner (who is responsible for the respective asset(s)?)	How is the Information Asset Ranked (5 high, 1 low) for Confidentiality, Integrity and Availability			Factored Rank (C*I*A)	C.I.A. on the scale of 1-5	General Value (from staff survey) 0= N/A, 1 is low; 5 is high				
			Confidentiality	Integrity	Availability			0	1	2	3	4
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
						0	0					
Examples												
Confidentiality	5	Usually for certain Customers and/or ABC_Company staff only										
	1	For public information										
Integrity	5	Must be 100% numerically accurate or unambiguous										
	1	Will tolerate a wide margin of error										
Availability	5	Must be available immediately										
	1	Should be available within 1 week										

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

- The risks to those assets and how they can be treated to keep them to an acceptable level

				Initial assessment						Assessment after treatment		
	Define this in words	Organisational role	Use 1 - 5 (1=low, 5=high)	Define this in words	How likely is this risk to occur? Use 1- 5 (1=low, 5=high)	How severe a problem is this risk if it occurs? Use 1- 5 (1=low, 5=high)	Multiply importance, probability and severity together, to derive a joint value	What are you going to do about this risk? □ Prevention □ Reduction □ Transference □ Contingency □ Acceptance	Controls to implement your risk treatment strategy.	Is this risk still likely to occur after treatment? Use 1- 5 (1=low, 5=high)	Will this risk still be as severe a problem if it occurs after treatment? Use 1- 5 (1=low, 5=high)	What is the expected risk after treatment has been implemented?
1							0%					0%
2							0%					0%
3							0%					0%
4							0%					0%
5							0%					0%
						Risk Factor	0%				Risk Factor	0%

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Appendix E. Internet threats[84]

Note: This is not a checklist! It is a list of examples to help you start compiling a risk register.

A member of a community carries out activities permitted only to those from that community with greater privileges

Appropriation, or copying of, company-sensitive information and master data files

Attacks against website data and information

Conflict of jurisdictions/applicable law

Data protection

Defacement of website

Defamation

Denial of service attack

Domain names

Extortion

Fraud

Ghost/spoof web sites

Identity theft

Internet browsing

Judgements vary as to whether liability is where the company is registered, the server computer is located, or where the user makes a purchase.

Mishandling of personal information – outside the 8 principles of data protection

Misrepresentation of authority

Physical appropriation of computer hardware or software

System crash by nuisance or criminal activity

System hijack for use as ‘Trojan Horse’

Theft (intangible assets)

Theft (tangible assets)

Theft of brand, cyber-squatting

Threat to reveal information culled from the Internet illegally or to post damaging information

Unlawful obtaining/use of personal information of another by fraud or deception, usually for financial gain

User action (fraud)

Using a computer to falsify corporate information for self-benefit

Using a computer to falsify corporate information for self-benefit

Using internal e-mail in disrespect to colleagues, customers, suppliers

Viewing/downloading illegal and other inappropriate material

Virus attack

Web sites that to all intents and purposes appear to belong to a legitimate business but are a front for defamation, fraudulent collection of confidential information etc.

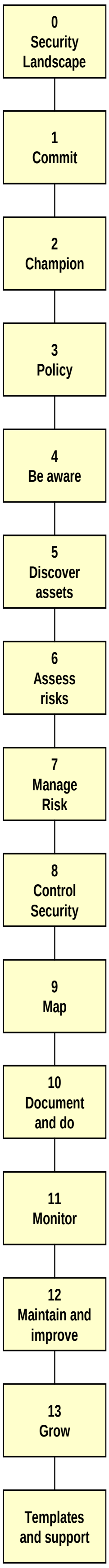
0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

[84] From the former National High Tech Crime Unit (NHTCU)

Appendix F. Internet application threats[85]

What penetration testers must look for . . .

Applications must be built so that these vulnerabilities are not created; refer to the *Information systems acquisition, development and maintenance* section of ISO/IEC 27002



Code Scanning — This is the simplest form of hack and in effect allows the malicious user to view the browser scripts thus allowing determination of where potential vulnerabilities exist.

Cookie Poisoning — Many web applications use cookies to save user information (user-id, timestamp, etc) on the client machine, this poses a potential opportunity for the malicious user:

- If cookies are not cryptographically secure, a hacker can modify them, thus fooling the application
- By changing the cookie values a malicious user can gain access to accounts that are not their own and subsequently generate transactions
- An attacker may also be able steal a user’s cookie and gain access to the user’s account without having to enter an ID and password or other form of authentication.

Hidden Manipulation — This is a specific form of parameter tampering that exploits hidden parameters and fields.

Hidden fields — Often used to save information about a client’s session and often hold data that has been retrieved from the back-end database. Despite their name, these fields can be viewed by performing a ‘View Source’ on a Web page. Many hackers take advantage of this by modifying hidden price fields and purchase items at little or no cost. This has been given the name ‘e-shoplifting’ and has obvious benefits to the hacker.

Forceful Site Browsing — Attempts to access URLs and pages that are normally only accessed through authentication mechanisms. As a result the Hacker may gain access, using this type of hack to URLs that could contain sensitive information.

Third Party Misconfigurations — Applications that contain insecure default settings or are configured insecurely by administrators. E.g. Web Servers, Application Servers, Content Management Systems, etc.

Known Vulnerabilities — This particular attack is all the more frustrating as it is based on utilising known component defects and problems that are in the public domain, an example of how even the most obvious of information can result in dramatic consequences. Known vulnerabilities include all defect and exploitable holes in the Operating System, Web server, application server, and other 3rd party web application components that have been published or are generally known.

[85] From ‘NCC Guideline 289: *Protect and Survive - Defending against application hacking*’

Buffer Overflow

It is the Buffer Overflow attack that has recently caused the ‘headlines’ especially in the case of the attacks against Microsoft. The malicious user sends more data than the application expects and thereby causes a buffer overflow. This causes an unpredictable application response and can cause the application to crash allowing the malicious user complete control.

The attacker uses this type of attack to try and crash the system or to gain complete control over it by having it execute the attacker’s malicious code. An example of this could be sending 500 characters to a 30-character Name field, or sending a large negative number (say -9999999) to a numeric Age field, etc.

Parameter Tampering

The manipulation of URL parameters to attempt to retrieve information that otherwise is not available to the user. This allows access to back-end databases if made through SQL calls that are often included in the URL. Malicious users can manipulate the SQL code to potentially retrieve a listing of all users, passwords, credit card numbers, or any other data stored in the database. These attacks are successful because most applications do not validate the returning web page server-side. This is an example where a development standard of ‘belt and braces’ validation and the use of re-usable code could remove this potential vulnerability across an application.

Stealth Commanding

Stealth Commanding is the ability to enter malicious Meta Characters within data input that will be executed by Server-Side applications. Examples of the type of characters (which have specific meanings to some operating systems) are: !@$%^&*()-_+’?/><{}[]~, ‘eval’ and ‘system’ Perl commands, server-side includes, and SQL queries enable hackers to plant Trojan-horses as form submissions and then run malicious or unauthorised code on the web-server, operating system or database servers.

Cross-Site Scripting

This is a process of inserting code into the page that will be viewed by another user. Using HTML forms and Cross-Site Scripting a malicious user could introduce executable code of his choice into another user’s web session. Once the code is running, it could take a wide range of actions, from monitoring the user’s web session to stealing session tokens of a valid user and sending them to the attacker.

Debug Options and Backdoors

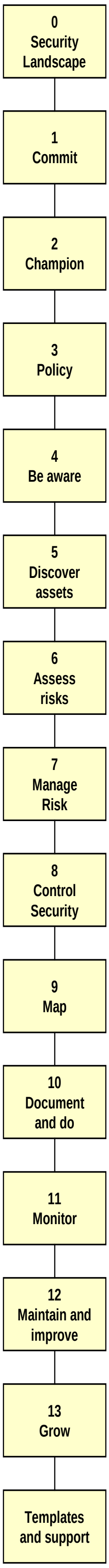
Developers often create Backdoors and Debugging features to aid testing and troubleshooting of web applications. Backdoors that allow a user to login with no password or access a special URL that allows direct access to application configuration are quite popular.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

SQL Injection

SQL Injection is a technique that permits an attacker to execute unauthorised SQL statements by manipulating data input into Web Applications by building dynamic SQL queries. An attacker could use SQL Injection to perform a large number of security attacks including:

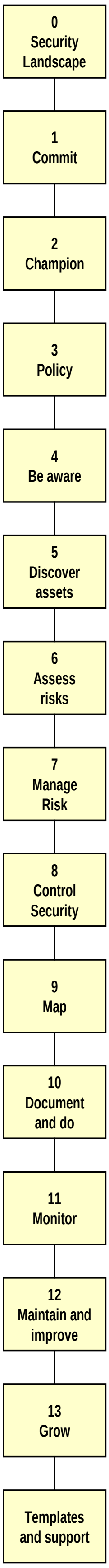
- Dropping all database tables
- Creating new tables
- Gain control of the database server
- Create user accounts to take control of the server hosting the database
- Gain unauthorised access to applications
- Gain access to confidential information, including credit card details and user authentication details
- Modify database data



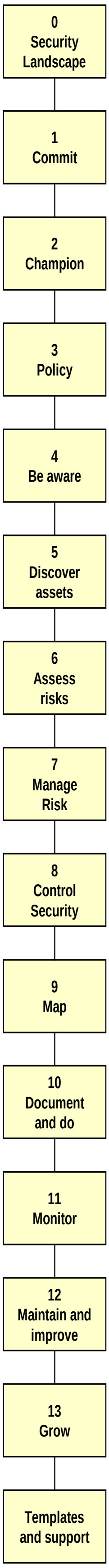
Appendix G. Contents of a business continuity plan

Here we have presented an amalgamation of headings from several good examples.

- Document control
  - Modification history – make it easy for stakeholders in the plan to see what’s changed.
  - Storage of the plan for accessibility in the event of an incident (include off-site-storage of the plan).
  - How the plan is kept up to date?
  - Distribution of plan so that the disaster recovery team are familiar with the latest version.
- Audits and rehearsals
  - How the efficacy of the plan is assured
  - Live or staged
  - Take lessons from incidents
  - Desktop walkthroughs
  - Major, minor, mixed incidents
  - Measure recovery times
  - End-to-end tests
- Key information assets
  - What the plan is protecting
- Key services
- Incident management - what happens when a problem occurs?
  - Responsibilities - the disaster recovery team - who does what?
  - Process in event of incident - a step-by-step guide to restoring information services.
  - Incident/action log - keeping track of what goes on for analysis and feedback to the business continuity plan.
  - Process at end of incident - how to round off the process and declare that operations have resumed.
- Disaster recovery team contacts - how are the key roles to be contacted, especially out of hours? Beware the implications of data protection. Home addresses and telephone numbers can be regarded as sensitive personal information.
- Prioritisation - how serious is the disaster? The imperative of the action taken should tally with the valuation of your information assets.
- How are emergency premises procured?
  - Parking
  - Staff facilities
  - Environment
  - Telephones
  - Electricity
  - Mail



  - Health and safety
  - Security
  - Staff transferred to continuity site (note: Business Interruption Insurance) including arrangements for:
  - Transport
  - Accommodation
  - Moving equipment in/out
  - Include computer systems recovery after relocation
- What are the contact details and processes to call up service contractors, suppliers, and maintenance companies?
- Disaster Recovery Plan.
  - How systems are organised
  - Solutions for minor incidents
  - Solutions for major incidents
  - Alternative strategies
  - Interim actions when off-line
  - Planning for ‘all’ potential disasters
  - cf. Levels of risk
  - Recovery of all computer systems including servers, workstations and desktop computers, and thin clients
  - May not cover physical relocation of company



Appendix H. A security oriented service level agreement

ISO/IEC 20000 recommends the basic components of an IT service level agreement whilst ISO/IEC 27002 includes a similar section which focuses on security. In this appendix we have combined the recommendations of both standards into single template. ISO/IEC 20000 is essential reading for the management processes to assure IT services.

1. Service

- A brief service description
  - A description of the product or service to be provided, and a description of the information to be made available along with its security classification
  - A clear and specified process of change management
  - The information security policy
  - References to supporting information such as a business continuity plan or accounting and budgeting documents
- Validity period and/or SLA change control mechanism
- Conditions for renegotiation/termination of agreements:
  - A contingency plan should be in place in case either party wishes to terminate the relation before the end of the agreements
  - Renegotiation of agreements if the security requirements of the organization change
- Service hours, for example, 09:00 h to 17:00 h, date exceptions (for example, weekends, public holidays), critical business periods and out of hours cover
  - The target level of service and unacceptable levels of service
- Service targets
  - The definition of verifiable performance criteria, their monitoring and reporting
- Asset management
  - Current documentation of asset lists, licences, agreements or rights relating to them.
  - Intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work
  - The right to monitor, and revoke, any activity related to the organization’s assets
  - Controls to ensure asset protection, including:

    (a) Procedures to protect organizational assets, including information, software and hardware

    (b) Any required physical protection controls and mechanisms

    (c) Controls to ensure protection against malicious software

    (d) Procedures to determine whether any compromise of the assets, for example, loss or modification of information, software and hardware, has occurred

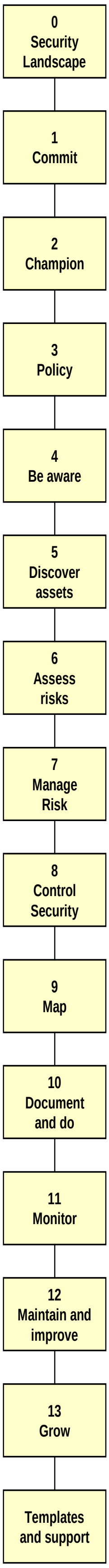
    (e) Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement

    (f) Confidentiality, integrity, availability, and any other relevant property of the assets

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

(g) Restrictions on copying and disclosing information, and using confidentiality agreements

- Workload limits (upper and lower), for example, the ability of the service to support the agreed number of users/volume of work, system throughput
  - The respective liabilities of the parties to the agreement
- High level financial management details, for example, charge codes etc
- Scheduled and agreed interruptions, including notice to be given, number per period
- Impact and priority guidelines
- Supporting and related services
- Any exceptions to the terms given in the SLA.
- Glossary of terms[86]



2. People

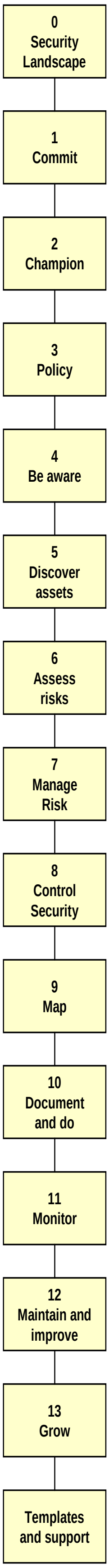
- Responsibilities
  - Customer responsibilities, for example, security
  - Service provider liability and obligations for example, security
  - Ensuring user awareness for information security responsibilities and issues
  - User and administrator training in methods, procedures, and security
  - Responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, for example, data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries
  - Responsibilities regarding hardware and software installation and maintenance
- The right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors
- Contact details of people authorized to act in emergencies, to participate in incidents and problem correction, recovery or workaround
- Arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement

3. Processes

- Authorization details
- Access control policy, covering:
  - The different reasons, requirements, and benefits that make the access by the third party necessary
  - Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords
  - An authorization process for user access and privileges
  - A requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use

[86] A glossary of terms may be held in one place, common to all documents

  - A statement that all access that is not explicitly authorised is forbidden
  - A process for revoking access rights or interrupting the connection between systems
- A brief description of communications, including reporting
  - A clear reporting structure and agreed reporting formats
  - Provision for the transfer of personnel, where appropriate
  - Involvement of the third party with subcontractors, and the security controls these subcontractors need to implement
- Housekeeping procedures
- Action to be taken in the event of a service interruption
  - Service continuity requirements, including measures for availability and reliability, in accordance with an organization’s business priorities
- Escalation and notification process
  - The establishment of an escalation process for problem resolution
- Complaints procedure



Appendix I. ISO cyber and information security standards

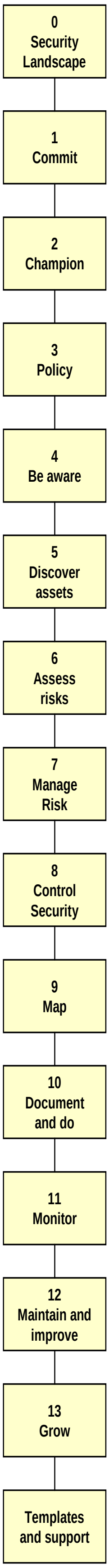
ISO/IEC 27000:2014	Glossary
ISO/IEC 27001:2013	ISMS requirements
ISO/IEC 27002:2013	ISMS controls…a code of practice
ISO/IEC 27003:2010	ISMS implementation guidance
ISO/IEC 27004:2009	Security metrics
ISO/IEC 27005:2011	Risk management
ISO/IEC 27006:2011	ISMS certification
ISO/IEC 27007:2011	ISMS auditing
ISO/IEC TR 27008:2011	Controls auditing guide
ISO/IEC 27009:TBA	Sector-specific ISMS
ISO/IEC 27010:2012	Information security management for inter-sector and inter-organisational communications
ISO/IEC 27011:2008 (ITU X.1051)	Information security management for telecommunications
ISO/IEC 27013:2015	Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014:2013	Information security governance
ISO/IEC TR 27015:2012	Information security management for financial services
ISO/IEC TR 27016	Information security management economics
ISO/IEC 27017	Information security controls for cloud computing
ISO/IEC 27018	Personal identifiable information on public cloud computing services
ISO/IEC TR 27019:2013	Information security for process control in the energy industry SCADA
ISO/IEC 27031:2011	ICT readiness for business continuity
ISO/IEC 27032:2012	Cyber security
ISO/IEC 27033:2009	IT network
ISO/IEC 27034:2011	Application security

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

ISO/IEC 27035:2011	Information security incident management
ISO/IEC 27036:2013	Supplier relationship management
ISO/IEC 27037:2012	Digital forensics
ISO/IEC 27038	Digital redaction
ISO/IEC 27039	Intrusion detection and prevention systems
ISO/IEC 27040	Storage security
ISO/IEC 27041	Suitability and adequacy of incident investigative methods
ISO/IEC 27042	Analysis and interpretation of digital evidence
ISO/IEC 27043	Incident investigation
ISO/IEC 27044	Security Incident and Event Management (SIEM)
ISO/IEC 27050	Electronic discovery
ISO 27799:2008	ISMS in the health sector

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support

Appendix J. Other information security standards



CESG 10 Steps to Cyber Security

This is a set of high level awareness guidance that centres on having a board's information risk management regime (step one) and nine things to implement it.

CPNI/SANS 20 Critical Controls for Cyber Defence

These are catalogue of controls set out by the USA's Center for Internet Security (CIS) and the SANS Institute which have been adopted by the UK's CPNI. They comprise a detailed set of activities commensurate with fighting 'most pervasive and dangerous attacks'. For an SME in particular, IASME provides the foundations for adopting these protective measures for high impact assets such as SCADA systems.

Cyber Essentials Scheme (CES)

Both IASME (see below) and the international standard ISO 27001 are based on a risk-led approach, with appropriate treatment. However, day-to-day information and cyber security risks are endemic within a wide range of organisations[87].

Cyber Essentials was created to mitigate the risk from common Internet-based threats based on a significant proportion of the everyday attack paths that lead to all organisations. It is deliberately prescriptive and is aimed to provide a base level of controls before the business even begins to work with computers and other information technology.

Cyber Essentials has similarities to the 'MOT' – a test of basic roadworthiness not mechanical assurance. Whereas Cyber Essentials is about the basic technology, IASME is about the technology, about you, *and about* where and how you work.

The IASME Standard for Information and Cyber Security

As the information age has matured, the rate of change – and complexity of business systems – has often left businesses vulnerable to information security breaches. Whereas there can be no guarantees for information safety, there are frameworks available to reduce the associated risks to an acceptable level. However, these frameworks often originate with a focus on large corporations where size and resources give them the wherewithal to implement the protective measures.

Smaller, dynamic businesses and organisations differ from their larger, more structured counterparts and must deal with information security with greater flexibility and with much smaller budgets. The structure of rigid procedures that support the internal communications in large organisations must give way to the informal cultures of small to medium-sized enterprises (SMEs).

Information Assurance for Small to Medium-sized Enterprises (IASME) is designed as a security benchmark for the SME. IASME is designed to guide the SME where needed and then assess the level of maturity of an SME's information security. Recognition of this benchmark can be used to assure themselves and their customers that information lodged with them is safe in all practical respects. IASME can also be scaled up for larger organisations.

IASME is an organised way for a business to implement new ways of securing its information, improve existing ones, and be recognised in its sector for having done so. Implementing IASME creates security-aware workers as a by-product.

IASME is programme of security assurance that has been compiled by SMEs for SMEs. It provides common ground for SMEs amongst other methods – or standards – which are either not comprehensive or are too prescriptive in their level of complexity for an SME.

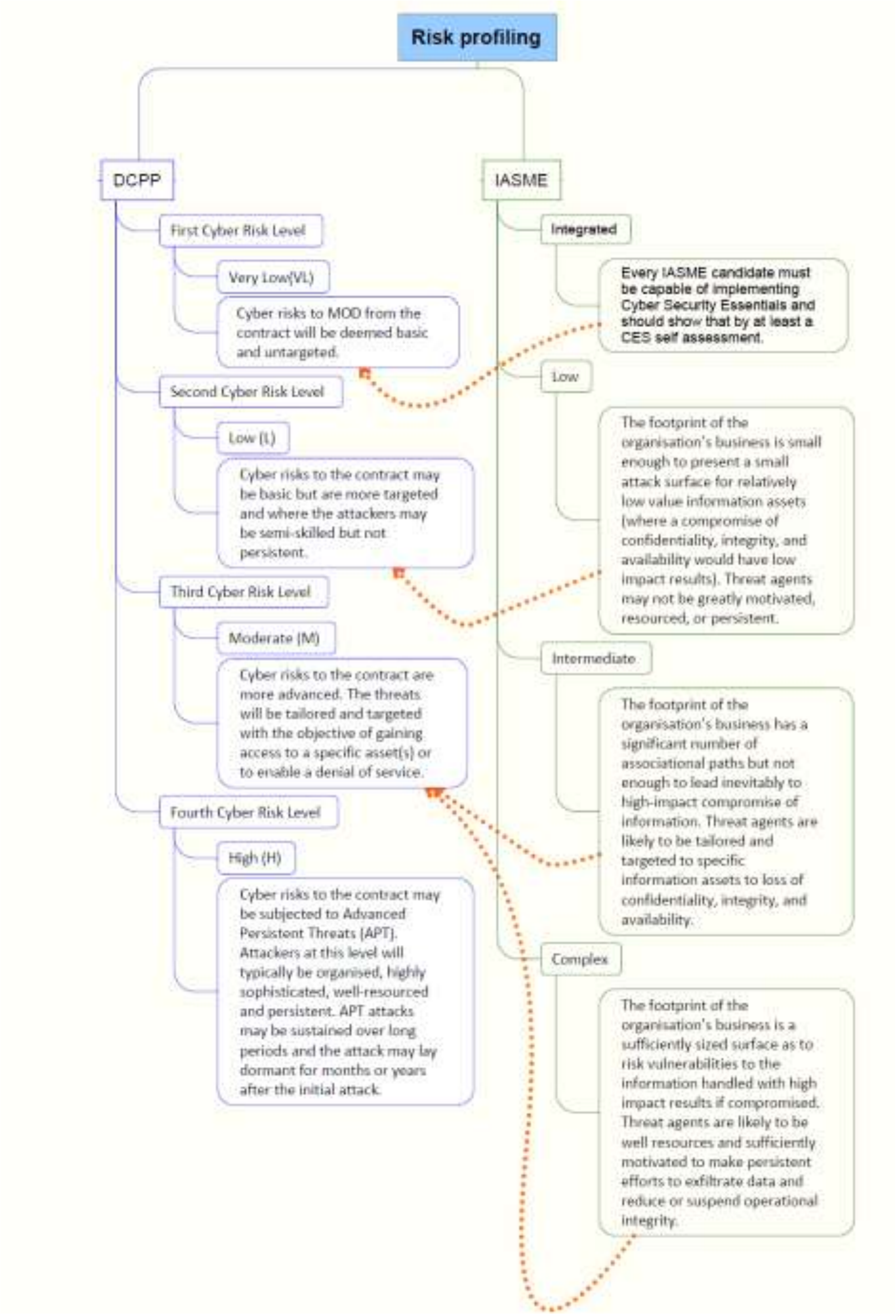
[87] See CESG (2015) *Common Cyber Attacks: Reducing The Impact*

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS compliance is mandated by the payment card suppliers for businesses handling payment card data. Like Cyber Essentials (*see 0.0.0.0 above*) it is essentially risk agnostic and says that if you handle payment card data, you must implement specific controls (as set out in that standard). Like DCPP (*see below*) and IASME, there is an element of risk profiling regarding the type of processing and storage that goes on in a business.

Defence Cyber Protection Partnership (DCPP) Cyber Risk Profiles

The IASME standard and the DCPP Cyber Risk Profiles specification (Defence Standard 05-138) have the common ground of basing the expected attention to security on the likely threats that risk the business' confidentiality, integrity, and availability.



Risk profiling

- DCPP
  - First Cyber Risk Level
    - Very Low(VL)
    - Cyber risks to MOD from the contract will be deemed basic and untargeted.
  - Second Cyber Risk Level
    - Low (L)
    - Cyber risks to the contract may be basic but are more targeted and where the attackers may be semi-skilled but not persistent.
  - Third Cyber Risk Level
    - Moderate (M)
    - Cyber risks to the contract are more advanced. The threats will be tailored and targeted with the objective of gaining access to a specific asset(s) or to enable a denial of service.
  - Fourth Cyber Risk Level
    - High (H)
    - Cyber risks to the contract may be subjected to Advanced Persistent Threats (APT). Attackers at this level will typically be organised, highly sophisticated, well-resourced and persistent. APT attacks may be sustained over long periods and the attack may lay dormant for months or years after the initial attack.
- IASME
  - Integrated
    - Every IASME candidate must be capable of implementing Cyber Security Essentials and should show that by at least a CES self assessment.
  - Low
    - The footprint of the organisation's business is small enough to present a small attack surface for relatively low value information assets (where a compromise of confidentiality, integrity, and availability would have low impact results). Threat agents may not be greatly motivated, resourced, or persistent.
  - Intermediate
    - The footprint of the organisation's business has a significant number of associational paths but not enough to lead inevitably to high-impact compromise of information. Threat agents are likely to be tailored and targeted to specific information assets to loss of confidentiality, integrity, and availability.
  - Complex
    - The footprint of the organisation's business is a sufficiently sized surface as to risk vulnerabilities to the information handled with high impact results if compromised. Threat agents are likely to be well resources and sufficiently motivated to make persistent efforts to exfiltrate data and reduce or suspend operational integrity.

0 Security Landscape
1 Commit
2 Champion
3 Policy
4 Be aware
5 Discover assets
6 Assess risks
7 Manage Risk
8 Control Security
9 Map
10 Document and do
11 Monitor
12 Maintain and improve
13 Grow
Templates and support