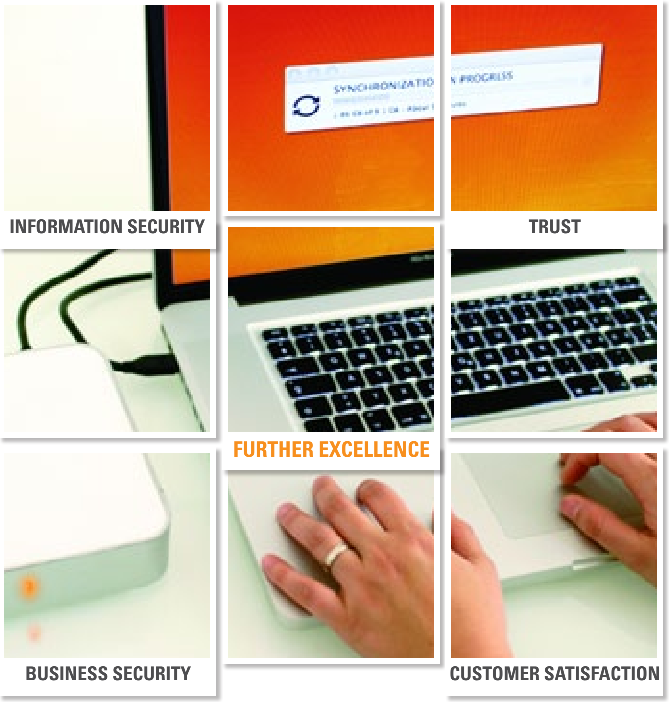
ISO/IEC 27001

THE STANDARD IN INFORMATION SECURITY MANAGEMENT



SGS

FOREWORD

"Today, business is driven by information. It is your most valuable asset.

Some information is public knowledge; some is private and of no real interest to others. But every organisation has some information which is confidential and of interest to others.

Confidential information can involve research, design, prototypes, key technologies, manufacturing methods, processes, marketing information, plans, forecasts, strategies and negotiating positions….

Information such as this could cause considerable damage if it fell into the wrong hands. This could have an immediate impact – for example, loss of a key contract. Or it could be more gradual, as you are overtaken by competitors which have short-circuited costly parts of the development process.

You may never realise that your information has been compromised. You simply find that you are inexplicably losing out."

Extract from: Protecting business information – Understanding the risks - DTI publication - URN 96/939.

BACKGROUND

This paper draws on the experience gained in working with public and private sector organisations successfully seeking to meet the demanding requirements for security in information and IT systems.

PURPOSE

SGS' objective is to inform and to summarise the principal requirements for guiding and establishing an information security policy and system.

This paper uses as a framework ISO/IEC 27001:2013 series - Specifications for information security systems.

Published by Systems and Services Certification. 2014

THE ROUTE TO ISO/IEC 27001

Issues to be considered when establishing an
Information Security Management System

AN INTRODUCTION TO ISO/IEC 27001:2013

In October 2005, the code of best practice outlined in BS 7799 was formally adopted by the International Standards Organisation as ISO/IEC 27001:2005. In October 2013 the standard was further updated to ISO/IEC 27001:2013. It has become internationally recognised as the standard for Information Security Management.

A number of changes have been made during this transition. ISO/IEC 27001:2013 has been aligned with the format of other management standards which have been subject to revision, e.g. ISO 22301 (the Business Continuity Management standard). As a result, ISO/IEC 27001:2013 has been documented to a common format, in accordance with Annex SL, with clauses 1-10 (rather than 1-8, as previously). Greater emphasis has been given to key areas such as management commitment and measurement of ISMS effectiveness, in order to encourage organisations to implement ISO/IEC 27001 within an overall strategy rather than in isolation.

THE STANDARD IS IN TWO PARTS:

ISO/IEC 27001 is the formal standard specification for an Information Security Management System (ISMS), against which an organisation seeking certification will be audited. The main body of the document provides a mandatory set of requirements that an organisation must meet for certification. An Appendix (Annex A) provides a list of control objectives that an organisation might use to measure information security. Controls relevant to an organisation should be selected based on a comprehensive risk assessment of the information security risks. With the publication of ISO/IEC 27001:2013, the number of clauses in Annex A has increased, from 11 in ISO 27001:2005, to 14 in ISO 27001:2013. The number of controls has decreased, from 133 in ISO 27001:2005, to 114 in ISO 27001:2013.

User defined controls can also be used, in addition to Annex A controls.

ISO/IEC 27002 provides a standard of good practice that may be applied to security of information and related assets.

There is no longer an explicit requirement for the ISMS process to be based on the plan-do-check-act (PDCA) model. However, Information Security Management is a continuous process, rather than a one-off project. Therefore it has to be based on an improvement model, which can be PDCA or another model of the organisation’s choosing.

TRANSITION FROM ISO/IEC 27001:2005 TO ISO/IEC 27001:2013

For organisations already certified to ISO/IEC 27001:2005, the process of transition should be relatively straightforward. Existing certificates will be replaced as part of the normal audit cycle, unless specifically requested.

SGS will commence issuing certificates to ISO/IEC 27001:2013 during 2014. Transition assessments of all SGS clients will have to be completed within one year of this process commencing.

WHO SHOULD READ THIS DOCUMENT?

The intended readership is:

- Executive management having responsibility for developing or leading information security policy
- Senior managers tasked with preparing or establishing information systems
- Professional advisors considering the relevance of information security to their own organisations or providing general advice to others
- IT service professionals involved in specifying and maintaining processing facilities and guiding applications development
- Medical professionals and managers
- Senior managers in central and local government and executive agencies.

CONVENTIONS USED IN THIS DOCUMENT:

1. Extracts or quotations are source identified and printed in *italic* typeface.
2. "'SGS' comments, based on client experience, are set out in *italic* typeface and are contained within quotation marks."

THE CASE FOR INFORMATION SECURITY

Technological development now means that globally based services can appear to be both national and local to the customer. For example, look no further than airline ticket reservations and telephone enquiry services. These trends are not confined to the private sector.

The UK is substantially a service based economy where design skills, knowledge of markets and information resources have considerable value.

Competitors, enabled by the adoption of e-commerce, are increasing the speed of response required and the value of know-how, in today's and tomorrow's marketplace.

Organisations that are not taking steps to safeguard their investment in information are at risk.

MANY ORGANISATIONS HAVE ESTABLISHED CONTROLS, RECOGNISING VULNERABILITIES AND GOOD PRACTICE, IN SUCH ACTIVITIES AS:

- Individual log-on and passwords for access to IT facilities
- Virus checking and IT back-up routines and off-site storage
- Tables of authorities – often financial or press statement related
- HR practices
- Complaints handling
- Business planning and disaster recovery/continuity arrangements
- IT fault reporting
- Guidelines for the use of e-mail, fax, internet and photocopiers
- Limitations to document or file access.

Such management actions represent a good start but are frequently compromised by poor discipline.

"We have seen frequent examples of passwords being written down and freely available to casual observers, insecure screen-savers and laptop computers being used for quite sensitive processing on trains and in public places. How often have you overheard inappropriate mobile telephone conversations and have almost been able to guess the other half of the dialogue?"

CIA

Organisational activity is rarely free from risk – this is certainly true when considering security of information. Information security is not about spy wars, but a disciplined management approach to preserving:

CONFIDENTIALITY:

preventing unauthorised access or disclosure

INTEGRITY:

safeguarding the accuracy and completeness of information and processing methods

AVAILABILITY:

ensuring that authorised users have access to information and associated processing methods when required. Loss of any of these attributes could, in certain circumstances, occasion commercial harm, embarrassment or serious business damage.

NOT ALL EQUALLY VALUABLE, OR VULNERABLE

Information security is not attained by paranoia, nor does it result from incomplete or partial thinking. The starting point, as in many management disciplines, is a comprehensive analysis and risk assessment.

Risks associated with loss of confidentiality, integrity and availability are to be identified, rather than the risk assessment being based on identifying assets and their associated threats and vulnerabilities. Threats and vulnerabilities are no longer referenced in ISO/IEC 27001:2013.

ISO/IEC 27001 – THIRD PARTY CERTIFICATION

Demonstrates clear evidence that an organisation may be considered a 'trusted trading partner' in matters of information security. It also encourages the suppliers to ensure continued compliance with the information security needs of their customers, and gives a framework for continual improvement.

RISK ASSESSMENT

Requires consideration of the organisational damage flowing from breach of confidentiality, integrity or availability and the likelihood that such a breach will occur and be exploited.

Comprehensive risk assessments are challenging tasks. There are sophisticated proprietary products available to assist these tasks but none is a substitute for top-level commitment, involvement of relevant staff and clarity of business objectives.

Applying the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the Information Security Management System may require external facilitation and expertise, particularly in complex IT issues.

THE RISK ASSESSMENT IS A DYNAMIC TOOL THAT SHOULD BE REVIEWED REGULARLY. IT IS RECOMMENDED THAT THIS BE A MINIMUM OF ONCE PER YEAR AND DEFINITELY WHEN THERE IS A BUSINESS CHANGE.

REMEMBER A DOCUMENTED RISK ASSESSMENT IS A RISK IN ITSELF AND MUST BE TREATED SECURELY.

RISK MANAGEMENT

Involves avoiding, reducing, accepting or transferring risks by adopting appropriate controls. The selection of controls needs to balance the costs and practicalities of operation, with the degree of risk reduction achieved.

ISO/IEC 27001 certification requires that a written "Statement of Applicability" shall identify and critique the controls selected and explain any exclusion.

Our experience is that currently, few organisations have addressed these requirements with sufficient rigour to meet third party certification requirements.

ESTABLISHING A MANAGEMENT FRAMEWORK

Necessitates defining the:

- Information security policy objectives
- Boundaries of the system, areas, assets, technology or other characteristics
- Conclusions of risk assessments
- Selection of controls
- Management responsibilities.

DOCUMENTATION AND CONTROL REQUIREMENTS

COMPRISE:

- Evidence of the risk assessment process
- Summary of the management framework
- Policy statements – e.g. clear desk, internet access, cryptography, access control etc.
- Specific operational and procedural documentation
- Management responsibilities and reviews
- Evidence of effectiveness
- Evidence of the monitoring and measurement of results.

Appropriate retention period, retrieval, version control, authorisation and ownership or accountability issues should be addressed.

"These requirements should present few difficulties to organisations familiar with ISO 9000 Quality Assurance Management disciplines."

AUTHORISING INFORMATION PROCESSING FACILITIES AND CHANGES TO OPERATIONAL FILES OR CONFIGURATION

The standard seeks formal technical and information security appraisal and authorisation for all new or changed operations.

"Many organisations will have in place procedures partially or fully addressing this requirement – particularly in IT areas. Review and strengthening may be required in non-IT functions."

SECURITY FORUM, CO-ORDINATION, SPECIALIST ADVICE AND INDEPENDENT REVIEW

The standard proposes establishing, where appropriate, a cross-functional forum, led by senior management, to provide co-ordination and visible support for information security.

Additionally, ISO/IEC 27001 requires that specialist advice (in-house or external) shall be sought and that implementation of information security policy shall be independently reviewed.

"For most organisations the requirement for independent advice and review, beyond the role of the legal and accountancy professions, will be new. With the pace of technological development, access to expert and independent views makes a good deal of sense.

Many organisations would need to address this issue."

THIRD PARTY ACCESS TO INFORMATION SYSTEMS

Most organisations set limitations to systems access, but how many will have considered the risks to information security arising from, say, cleaning staff and waste disposal methods?

All contracts with service providers, including IT maintenance and outsourcing, should be assessed for risks and suitable controls and defined, operated, and clear responsibilities incorporated into contract terms.

"Agreements with suppliers shall include requirements to address the information security risks."

INFORMATION PROCESSING ASSET INVENTORIES AND CLASSIFICATION

Inventories of physical assets indicating location and ownership are routine. Inventories of databases, processing methods and technologies are rarer.

"In our experience, information database inventories are rarely accompanied by classification and labelling indicating importance and handling sensitivity."

PERSONNEL ISSUES

ISO/IEC 27001 seeks to build on current good recruitment practices, by ensuring that information security responsibilities are incorporated in terms and conditions of employment and that security education forms part of all employee and temporary staff induction programmes.

"For sensitive information handling, consideration should be given to screening of potential employees, checking of CVs and the desirability of enforceable confidentiality agreements."

DETECTION, REPORTING AND HANDLING SECURITY INCIDENTS AND PROCESSING MALFUNCTIONS

Clearly not all incidents are harmful. Some will arise from the identification of weaknesses or of potential threats. Others will arise from breakdown or fault with hardware. Procedures should be developed for classification and handling incidents and for containment, corrective action and damage limitation.

DISCIPLINARY CODE

Should be invoked for wilful violation of security policy. This may require renegotiation of existing disciplinary practices.

PHYSICAL, ENVIRONMENTAL AND EQUIPMENT SECURITY

There are many important and practical issues to be considered:

- Isolated delivery areas
- Failover/multiple power supplies
- Physical perimeters
- Office/room security
- Equipment siting
- Cabling security
- Equipment maintenance
- Access control devices
- Disposal or reuse of media or equipment

- Off-site equipment
- Cleaning/canteen
- Location identification
- Working in secure areas
- Duress alarms
- Separation of development and operational activities
- Segregation of power and data cabling.

"Specialist advice may be required when considering the risk reduction and management benefits of implementing several of these control options."

GENERAL CONTROLS

The standard includes good practice general controls such as:

- Secure screen savers and clear desk policies
- Regular virus checking and authorised software audits
- Property removal authorisation and control
- Segregation of duties and authorities
- Review and authorisation of operational change – facilities, software versions or processing venues
- Regular back-up disciplines with off-site storage and other good housekeeping disciplines.

SYSTEMS PLANNING, SPECIFICATION AND ACCEPTANCE

A readily understood risk of security compromise arises through inadequately or inappropriately specified hardware or application software. Systems that regularly ‘crash’ place strains on staff, promote extra and usually hurried work and encourage the taking of short-cuts, with inevitable risks.

“ISO/IEC 27001 requires systems capacity planning, formal specification and acceptance criteria to be established for all new or upgraded hard/software.”

MEDIA HANDLING AND SECURITY

Applies to items such as paper, tapes, discs, and other forms of electronic media, lists of assets, systems documentation and procedures.

Compliance is largely a matter of common sense in preserving such items free from corruption, unauthorised change and readily available when required.

“It is surprising how many important items continue to go missing through inadequate storage and handling disciplines. Newspaper stories of confidential files found on hard discs and surplus or old equipment underline the need for controls in both handling and disposal.”

INFORMATION OR SOFTWARE EXCHANGES

The number of partnership, joint ventures or shared data access trading relationships has increased rapidly. E-commerce is now widely used by central government and service providers. E-mail is the standard way of communicating in many organisations. Internet access is widely available in public places, and via mobile networks.

These developments have one thing in common: the sharing of information is getting much easier and faster.

It would be consoling to think that the suppliers and/or third parties involved in these transactions share your concerns for information security, or are aware of the risks of external interception, eavesdropping or message redirection. Even in the closest of trading relationships, duplication or change of data can occur – possibly arising through the use of temporary staff.

"Standard office software contains powerful code writing features and other capabilities that the inquisitive can invoke. Have these features been disabled in your organisation?

In our view and that of ISO/IEC 27001, all information transfers: exchanges of information or software access should be regulated by written agreements, and external network access should be subject to guidance and control."

USER ACCESS MANAGEMENT AND RESPONSIBILITIES

Issues to be addressed include:

- Documenting an access control policy that is aligned to organisational business needs
- Formal user registration and deregistration procedures
- Log-on and privilege restriction routines
- Password disciplines – using regularly changed high quality passwords
- User adherence to password protection and change procedure
- Regular review of access rights
- Policies in place covering emerging risks, e.g. employee's use of their own devices for work related tasks

"It is commonplace that passwords are:

Easily guessed

Often written down and readily retrievable

Not changed frequently."

ACCESS TO NETWORK CONTROLS

Any review of information security would be incomplete without considering controls on:

- User authentication for all remote users – e.g. use of two-factor authentication
- Network controls
- Segregation in networks
- Security of network services.

"A documented network security policy should be prepared addressing these and related issues."

OPERATING SYSTEM CONTROLS

These are linked to network access controls and are intended to prevent unauthorised access to operational systems. They include:

- Automatic terminal identification to specific locations, users and portable equipment
- Tight restriction of access to system utilities
- Controls against malware
- Rigorous operating system change authorisation and control.
- Restrictions on software installation.

"Unregulated change is one of the largest causes of compromise to an initially sound system security control."

SYSTEM MONITORING

Automated event logging provides a means of tracking:

1. User access and application requests granted and denied
2. Capacity utilisation
3. Other system environment attributes.

When integrated with ‘clock synchronisation’ such logs provide valuable audit trails for review and evidence of effective operation.

MOBILE DEVICES AND TELEWORKING

The growth of remote working creates additional information security risks that should be considered in a formal policy covering:

- Guidance on use of file or message content
- Protection against theft of hardware and media
- Back-up disciplines for mobile computing
- Access to public networks
- Access to organisation networks with additional controls for remote location access
- Restrictions on file downloading
- Security at fixed teleworking locations
- Encryption of transmissions and storage media.

“Technology supports the practicality of a mobile office. Unfortunately security is much harder to ensure and monitor in off-site conditions.”

INFORMATION DATA AND PROCESSING CONTROL

ISO/IEC 27001 consolidates good management practices such as:

- Secure development policy
- Secure system engineering principles
- System security testing.

ENCRYPTION AS A SECURITY MEASURE

Cryptographic techniques are the subject of legal and proprietary regulation. A distinction should be drawn between the widely used e-mail file transmission encoding techniques and full cryptographic security controls.

Cryptography use should be set out in a policy that safeguards the organisation’s:

- Legal use
- Encryption algorithms
- ‘Key’ management and security
- Use of digital signatures authenticating information transmissions
- Contractual implications of digital signatures and of information transmission and receipt acknowledgement
- Internal fiduciary authorities/accountabilities.

“This is an aspect of information security that, in our experience, requires inputs from professional advisors and specialist crytography advice.”

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

The continuity of information security in business needs to be a core organisational requirement. Procedures for developing and maintaining the continuity of security should be established taking account of organisational objectives and appropriate risk assessments.

Information security continuity requirements include the planning, implementation, and evaluation of continuity arrangements.

The challenge posed by estimating the effects of a major breach of information security could have implications for:

- Safety of personnel
- Financial penalty
- Breach of legislation or regulation
- Loss of business confidence and reputation.

"We have reviewed and commented upon a number of Information security continuity plans which have been developed in a piecemeal manner. These plans generally lack the single co-ordinating framework required to be effective and to meet ISO/IEC 27001 requirements."

LEGAL AND REGULATORY COMPLIANCE

Organisations operate within a background of legislation and specific regulation by trade and professional associations. A few examples of general legislation are:

- Data Protection Act (1998)
- Data Protection (Processing of Sensitive Personal Data) Order (2000)
- Regulation of Investigatory Powers Act (2000)
- Criminal Justice and Public Order Act (1994) – electronic media storage
- Computer Misuse Act (1990)
- Copyright, Designs and Patents Act (1988)

- Obscene Publications Act (1959)
- Wireless Telegraphy Act (1949).

Complying with all relevant law is an inescapable obligation on all and is intrinsic to meeting the obligations of ISO/IEC 27001.

Procedures should be operated to authorise the use of information processing and storage facilities and to prevent misuse. Such procedures should be supported by regular audits of all software and data stored on system networks and free–standing equipment both on and off-site.

Where actions against persons or the organisation involve possible criminal, civil or regulatory hearings, evidence should be collected in accordance with relevant law or codes of practice, for admission.

COMPLIANCE WITH SECURITY POLICY AND PROCEDURES

Irrespective of a decision to seek third party ISO/IEC 27001 certification, audit of adherence to the organisation's security policy is an essential discipline. Internal audit, independent external review and advice are fundamental to any effective system. It also gives a means of providing evidence of compliance and identifying improvement opportunities.

Essential components of demonstrating compliance are:

- Safeguarding and readily retrievable records
- Secure keeping of test data used to verify operational integrity and assess acceptance criteria for new or upgraded systems
- Records dealing with security incidents
- Technical specification and risk assessments
- Protection of system audit tools
- The stature, training and independence of internal auditors and their access to senior management
- Information security procedure documentation including lists of system assets and operational configuration.

"Many of the compliance evidencing issues will be familiar to organisations already meeting ISO 9001 requirements, although the extension to security audit tools may be new."

Requests for additional copies of this paper, or for further information on ISO/IEC 27001 certification, should be directed to SGS United Kingdom Ltd.

ACHIEVING ACCREDITED CERTIFICATION

After implementing an Information Security Management System, many organisations then go through the process of obtaining accredited certification. This enables them to make a public statement that they are serious about the confidentiality, integrity and availability of their information and that of their clients.

The certification also enables organisations to provide evidence in response to security questions in tenders and other commercial contracts without the need to divulge confidential security policy and procedures.

In the UK the accreditation body for certification bodies is UKAS. The United Kingdom Accreditation Service is the sole national accreditation body recognised by government. For more information visit: www.ukas.co.uk.

If you are considering obtaining certification it is worth contacting SGS at the early stages of the project. One of SGS' core beliefs is to understand the needs and objectives of its clients so that the best possible service can be provided and to develop long term relationships.

In an initial consultation SGS can give you budget costing for achieving certification, advise on scope and statement of applicability as well as ensuring its certification audits fit within your project plan.

It's worth noting that the SGS code of ethics forbids SGS from undertaking consultancy where it also provides certification services. This ensures that SGS' opinions are unbiased.

STAGES

1. Initial consultation to develop budget costs and timescales
2. Formal proposal
3. Application
4. Pre-assessment: an optional audit to ascertain the client's readiness to move towards certification
5. Desk study – an appraisal of the client's information security manual/procedures, risk assessment and statement of applicability to measure compliance with the standard and prepare working documentation for the on-site assessment. Any identified areas of non-compliance at this stage will be notified to the client so that where possible corrective actions can be taken before the on-site audit
6. On-site certification audit – an assessment to verify the implementation of your documented Information Security Management System
7. Reporting and closing of any corrective action requests
8. Certification – The client is notified of formal certification against ISO/IEC 27001, and a certificate is issued
9. Continuous Assessment – The certificate is valid for three years, during which time SGS will undertake regular assessment audits. The timing and frequency of these will be detailed in the initial proposal. Towards the end of the three-year period SGS will undertake a certification renewal. This is a more detailed audit than an assessment audit and takes account of systems changes.

Greater detail on the process, reporting and corrective action requests, can be found in SGS' document "Certification Process explained", which can be obtained by contacting SGS.

SGS can also offer a number of training courses to assist an organisation throughout the process: visit www.sgs.co.uk/training.

THE SGS GROUP

SGS is the world's leading inspection, verification, testing and certification company. SGS is recognised as the global benchmark for quality and integrity. With more than 80,000 employees, SGS operates a network of over 1,650 offices and laboratories around the world.

SGS can support you in opening up new business opportunities with security conscious customers. Using our experience and expertise we deliver results and analysis in a concise, clear and meaningful format; and make recommendations for action plans on any issues arising with dealers to ensure the improvement of your business.

Enhancing processes, systems and skills is fundamental to your ongoing success and sustained growth. We enable you to continuously improve, transforming your services and value chain by increasing performance, managing risks, better meeting stakeholder requirements, and managing sustainability.

With a global presence, we have a history of successfully executing large-scale, complex international projects. Our people speak the language, understand the culture of the local market and operate globally in a consistent, reliable and effective manner.

For more information, please contact:

SGS United Kingdom Ltd
Systems & Services Certification
SGS House
217-221 London Road
Camberley
Surrey
GU15 3EY
United Kingdom

Tel: 0800 900 094
Fax: +44 (0)1276 697 696
email: uk.nowisthetime@sgs.com
web: www.sgs.co.uk/ISO27001

WWW.SGS.COM
WWW.SGS.CO.UK

WHEN YOU NEED TO BE SURE

SGS