Secure confidence

ISSUES TO BE CONSIDERED WHEN ESTABLISHING AN INFORMATION SECURITY MANAGEMENT SYSTEM

SGS

Introduction

FOREWORD

‘Keeping sensitive company information and personal data safe and secure is not only essential for any business but a legal imperative. Many organizations do this with the help of an information security management system (ISMS).

In an age of increasing data usage and the risk of information security breaches and cyber-attacks, the benefits of an ISMS are clear. Not only can it help to minimize the chance of such breaches occurring, it can reduce the costs associated with keeping information safe.’

Extract from: Guidance for ISMS Auditors just updated
International Organization for Standardization – 27 January 2020

BACKGROUND

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

AN INTRODUCTION TO ISO/IEC 27001:2013

ISO/IEC 27001:2013 is globally recognized as the standard for Information Security Management.

An Information Security Management System (ISMS) is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

The objectives of the standard are to:

- Examine risk to company information security and implement controls (policies, procedures, treatments) to manage the risks
- Manage threats to information assets
- Establish, maintain and continually improve an effective Information Security Management System (ISMS)

ISO/IEC 27001:2013 is documented in a common format in accordance with Annex SL, with clauses 4–10 that align with other ISO standards such as ISO 9001:2015 and ISO 14001:2015.

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 bold typeface and are contained within quotation marks."

THE STANDARD IS IN TWO PARTS

ISO/IEC 27001 is the formal standard specification for an Information Security Management System (ISMS), against which an organization seeking certification will be audited.

The main body of the document provides a mandatory set of requirements that an organization must meet for certification. An appendix (Annex A) provides a list of 114 controls that an organization may use to measure information security. Controls relevant to the organization are selected based on a comprehensive risk assessment of the information security risks.

In addition, ISO/IEC 27002 provides guidance and good practice that may be applied to implementation of these Annex A controls, to ensure security of information and related assets.

How ISO 27001:2013 helps

THE BENEFITS OF ISO 27001:2013 INCLUDE:

- Demonstrates that your organization keeps confidential information secure
- Increases customer, third-party and stakeholder confidence in how your organization manages risk
- Increases customer, third-party and stakeholder confidence that their data is protected, accessible and stored securely
- Help secure new business by meeting tender requirements and enhancing the organization's credibility
- Differentiates your organization against competitors
- It is a customer requirement in many European countries and is a prerequisite for most tenders for contracts
- Safeguards your valuable data and intellectual property
- Confirms you are meeting legal, contractual and regulatory requirements
- Manages and minimizes risk exposure – helps avoid financial penalties for data breaches

> **"THESE REQUIREMENTS SHOULD PRESENT FEW DIFFICULTIES TO ORGANIZATIONS FAMILIAR WITH ISO 9000 AND ISO 14001 MANAGEMENT DISCIPLINES."**

CIA

Organizational activity is rarely free from risk – this is certainly true when considering security of information. Information security requires a disciplined management approach to preserving:

CONFIDENTIALITY:

Preventing unauthorized access or disclosure

INTEGRITY:

Safeguarding the accuracy and completeness of information and processing methods

AVAILABILITY:

Ensuring that authorized 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.

NODE 01
NODE 04
NODE 05
BLOCK 01
mirror_mod.use_x
mirror_mod.use_y
mirror_mod.use_z = True
selection at the end -add
ob.select= 1
bpy.context.selected_o
data.objects[one.name]
print("please select exac

Manage risk

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.

ISO/IEC 27001 – THIRD-PARTY CERTIFICATION

Demonstrates clear evidence that an organization 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 organizational 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.

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.

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

ESTABLISHING A MANAGEMENT FRAMEWORK

Necessitates defining the:

- Scope of certification
- Information security policy objectives
- Boundaries of the system, areas, assets, technology or other characteristics
- Results of risk assessments and their treatment
- Selection of controls
- Management responsibilities

DOCUMENTATION CONTROL REQUIREMENTS

Comprises:

- 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, authorization and ownership or accountability issues should be addressed

"Typical issues relating to ISMS document management can include:

- Producing too much documentation
- Documentation too technical/high level
- Documentation does not cover all requirements
- Documentation update process not in place
- Documentation repository does not meet requirements"

"ISO/IEC 27001 CERTIFICATION REQUIRES THAT A WRITTEN 'STATEMENT OF APPLICABILITY' SHALL IDENTIFY AND CRITIQUE THE CONTROLS SELECTED AND JUSTIFY THE REASONS FOR THEIR INCLUSION AND EXCLUSION. OUR EXPERIENCE IS THAT CURRENTLY, FEW ORGANIZATIONS HAVE ADDRESSED THESE REQUIREMENTS WITH ENOUGH RIGOUR TO MEET THIRD-PARTY CERTIFICATION REQUIREMENTS".

Management buy-in and raising staff awareness

Obtaining Management buy-in and ensuring all staff are aware of the organization's ISMS and their associated information security responsibilities can be a challenge:

TOP MANAGEMENT

Need to align business strategy to meet the organization's strategic objectives

Cultural change is required and driven by buy-in from all senior managers

Ensure that there is a detailed communication plan

Ensure there are defined roles and responsibilities for all staff

STAFF AWARENESS

Ensure that staff are kept involved in the development of the ISMS and are informed of any required changes

Appoint representatives from internal departments and/or teams

Create Information security awareness training to cover all required aspects of the ISMS

Awareness of information security policies and procedures

NODE 05

Secure information

AUTHORIZING INFORMATION PROCESSING FACILITIES AND CHANGES TO OPERATION FILES OR CONFIGURATION

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

“MANY ORGANIZATIONS WILL HAVE IN PLACE PROCEDURES PARTIALLY OR FULLY ADDRESSING THIS REQUIREMENT – PARTICULARLY IN IT AREAS. REVIEW AND STRENGTHENING MAY BE REQUIRED IN SOME NON-IT FUNCTIONS.”

THIRD-PARTY ACCESS TO INFORMATION SYSTEMS

Most organizations 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.”

Secure information

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."**

HR SECURITY

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; there are processes in place for onboarding staff and for leavers; and that security education forms part of all employee and temporary staff induction programmes.

Disciplinary code can be invoked for wilful violation of information security policies. This may require renegotiation of existing disciplinary practices.

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.

Learning from security incidents is also an important part of the process.

> **"FOR SENSITIVE INFORMATION HANDLING, CONSIDERATION SHOULD BE GIVEN TO SCREENING OF POTENTIAL EMPLOYEES, CHECKING OF CVS, REMOVAL OF LEAVER ACCESS AND ASSOCIATED RECORDS AND THE DESIRABILITY OF ENFORCEABLE CONFIDENTIALITY AGREEMENTS."**

PHYSICAL, ENVIRONMENTAL AND EQUIPMENT SECURITY

There are many important and practical issues to be considered related to physical security controls. These can include:

- Physical security perimeter
- Physical entry controls
- Office/room security
- Protecting against external and environmental threats
- Equipment siting
- Working in secure areas
- Delivery and loading areas
- Cabling security
- Equipment maintenance records
- Access control devices
- Disposal or reuse of media or equipment
- Unattended user equipment
- Clear desk and clear screen policy
- Off-site equipment
- 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 authorized software audits
- Property removal authorization and control
- Segregation of duties and authorities
- Review and authorization 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."**

Secure systems

MEDIA HANDLING AND SECURITY

Applies to items such as paper, tapes, disks, 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, unauthorized change and readily available when required. The objective is to stop unauthorized release, alteration, deletion, or destruction of information contained in the media.

"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 DISKS AND SURPLUS OR OLD EQUIPMENT UNDERLINE THE NEED FOR CONTROLS IN BOTH HANDLING AND DISPOSAL."

INFORMATION OR SOFTWARE EXCHANGE

The number of partnerships, joint ventures or shared data access trading relationships has increased rapidly. Email is the standard way of communicating in many organizations. 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 by using 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 ORGANIZATION? IN OUR VIEW AND THAT OF ISO/IEC 27001, 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."

Secure systems

OPERATING SYSTEM CONTROLS

These are linked to network access controls and are intended to prevent unauthorized 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 authorization and control
- Restrictions on software installation

"UNREGULATED CHANGE IS ONE OF THE LARGEST CAUSES OF COMPROMISE TO AN INITIALLY SOUND SYSTEM SECURITY CONTROL."

USER ACCESS MANAGEMENT AND RESPONSIBILITIES

Issues to be addressed include:

- Documenting an access control policy that is aligned to organizational 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. employees' use of their own devices for work related tasks
- Only allowing passwords of adequate length
- Requiring users to re-enter their password after a period of inactivity
- Use secure password repositories

"Common issues encountered include passwords that are:

- Easily guessed
- Written down and readily retrievable
- Shared between employees

"A DOCUMENTED NETWORK SECURITY POLICY SHOULD BE PREPARED ADDRESSING THESE AND RELATED ISSUES."

- Not changed frequently.
- Saved in unsecure spreadsheets/documents”

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

SYSTEM MONITORING

Automated event logging provides a means of tracking:

- User access and application requests granted and denied
- Capacity utilization
- Other system environment attributes

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

MOBILE DEVICES AND TELEWORKING

The growth of remote/home 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 organization 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. HOWEVER, INFORMATION SECURITY IS MUCH HARDER TO ENSURE AND MONITOR IN OFF-SITE CONDITIONS.”**

Secure compliance

ENCRYPTION AS A SECURITY MEASURE

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

Cryptography use should be set out in a policy that safeguards the organization'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

"THIS IS AN ASPECT OF INFORMATION SECURITY THAT CAN REQUIRE INPUTS FROM PROFESSIONAL ADVISORS AND SPECIALIST CRYPTOGRAPHY ADVICE."

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

The continuity of information security in business needs to be a core organizational requirement. Procedures for developing and maintaining the continuity of security should be established taking account of organizational 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 THAT 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."

Secure compliance

LEGAL AND REGULATORY COMPLIANCE

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

- General Data Protection Regulation (GDPR)
- Computer Misuse Act
- Copyright, Designs and Patents Act
- Official Secrets Act
- Education Act
- Equality Act
- Freedom of Information Act
- Data Protection Act 2018

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 authorize 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 organization 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 organization'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

> **"MANY OF THE COMPLIANCE EVIDENCING ISSUES WILL BE FAMILIAR TO ORGANIZATIONS ALREADY MEETING ISO 9001 AND ISO 14001 REQUIREMENTS, ALTHOUGH THE EXTENSION TO SECURITY AUDIT TOOLS MAY BE NEW."**

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

ACHIEVING ACCREDITED CERTIFICATION

After implementing an Information Security Management System, many organizations 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 organizations 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 recognized by government. For more information visit: www.ukas.com.

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 is 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.

Path to certification

SGS can also offer a number of training courses to assist an organization throughout the process.

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 Stage 1 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 Stage 2 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.

SGS group

THE SGS GROUP

SGS is the world's leading inspection, verification, testing and certification company. SGS is recognized as the global benchmark for quality and integrity. With more than 94,000 employees, SGS operates a network of over 2,600offices 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.

WHY USE SGS?

Established in 1878, we are now the largest assessment and certification company in the world, with resources to match even the most demanding global contracts.

We strive to help you maintain certification year after year by offering opportunities for improvement, way beyond that of our competition. Our auditor training is one of the industry's strictest sign-off pathways – our clients receive the most qualified/trained auditors.

Our audit teams are multiskilled and carry out Integrated Management System audits covering a wide range of ISO standards as well as being consistently rated highly, which is evident from our most recent customer survey that produced the following results:

- 85% of respondents were satisfied with auditors' knowledge
- 86% of respondents were very satisfied with the auditor communication – confirming their audit was clear, open-minded and informative
- 90% of respondents were very satisfied with timeline for delivery of the audit report
- 94% of respondents felt very satisfied that the site visit was structured well to suit their operations

SGS are UKAS accredited and this entails the following advantages:

- Minimizes risk
- Saves money
- Enhanced reputation
- Opens opportunities
- Decreased potential product failure
- International recognition

For more information please contact:
SGS United Kingdom Ltd
SGS House
217-221 London Road
Camberley
Surrey
GU15 3EY
United Kingdom
Tel: +44 (0)1276 697715
Email: uk.nowisthetime@sgs.com
Website: www.sgs.co.uk/ISO27001

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

SGS