nqa.

ISO 27001:2013

INFORMATION SECURITY IMPLEMENTATION GUIDE

nqa.

> ISO 27001:2013

IMPLEMENTATION GUIDE

*UK and Ireland only

Contents

INTRODUCTION TO THE STANDARD

Most businesses hold or have access to valuable or sensitive information. Failure to provide appropriate protection to such information can have serious operational, financial and legal consequences. In some instances, these can lead to a total business failure.

The challenge that most businesses struggle with is how to provide appropriate protection. In particular, how do they ensure that they have identified all the risks they are exposed to and how can they manage them in a way that is proportionate, sustainable and cost effective?

ISO 27001 is the internationally-recognised standard for Information Security Management Systems (ISMS). It provides a robust framework to protect information that can be adapted to all types and sizes of organization. Organizations that have significant exposure to information-security related risks are increasingly choosing to implement an ISMS that complies with ISO 27001.

The 27000 Family

The 27000 series of standards started life in 1995 as BS 7799 and was written by the UK's Department of Trade and Industry (DTI). The standards correctly go by the title "ISO/IEC" because they are developed and maintained jointly by two international standards bodies: ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission). However, for simplicity, in everyday usage the "IEC" part is often dropped.

There are currently 45 published standards in the ISO 27000 series. Of these, ISO 27001 is the only standard intended for certification. The other standards all provide guidance on best practice implementation. Some provide guidance on how to develop ISMS for particular industries; others give guidance on how to implement key information security risk management processes and controls.

Three of the standards are particularly helpful to all types of organizations when implementing an ISMS. These are:

- **ISO 27000 Information Technology – Overview and vocabulary**
- **ISO 27002 Information technology – Security techniques** – Code of practice for information security controls. This is the most commonly referenced, relating to the design and implementation of the 114 controls specified in Annex A of ISO 27001.
- **ISO 27005 Information Technology – Security techniques** – Information security management.

Regular reviews and updates

ISO standards are subject to review every five years to assess whether an update is required.

The most recent update to the ISO 27001 standard in 2013 brought about a significant change through the adoption of the "Annex SL" structure. While there were some very minor changes made to the wording in 2017 to clarify the requirement to maintain an information asset inventory, ISO 27001:2013 remains the current standard that organizations can achieve certification to.

BENEFITS OF IMPLEMENTATION

Information security is becoming increasingly important to organizations, and the adoption of ISO 27001 therefore more and more common. Most organizations now recognise that it is not a question of if they will be affected by a security breach; it is a question of when.

Implementing an ISMS and achieving certification to ISO 27001 is a significant undertaking for most organizations. However, if done effectively, there are significant benefits for those organizations that are reliant on the protection of valuable or sensitive information. These benefits typically fall into three areas:

COMMERCIAL

Having independent third-party endorsement of an ISMS can provide an organization with a competitive advantage, or enable it to 'catch up' with its competitors. Customers that are exposed to significant information security risks are increasingly making certification to ISO 27001 a requirement in tender submissions. Where the customer is also certified to ISO 27001 they will, in the medium term, choose to work only with suppliers whose information security controls they have confidence in and that have the capability to comply with their contractual requirements.

For organizations that want to work with this type of customer, having an ISO 27001 certified ISMS is a key requirement for sustaining and increasing their commercial revenues.

OPERATIONAL

The holistic approach of ISO 27001 supports the development of an internal culture that is alert to information security risks and has a consistent approach to dealing with them. This consistency of approach leads to controls that are more robust in dealing with threats. The cost of implementing and maintaining them is also minimised, and in the event of them failing the consequences will be minimised and more effectively mitigated.

PEACE OF MIND

Many organizations have information that is mission-critical to their operations, vital to sustaining their competitive advantage or an inherent part of their financial value. Having a robust and effective ISMS in place enables business owners and managers with responsibility for managing risks to sleep easier at night knowing that they are not exposed to a risk of heavy fines, major business disruption or a significant hit to their reputation.

In today's knowledge-based economy, almost all organizations are reliant on the security of key information. Implementation of a formal ISMS is a proven method of providing such security.

ISO 27001 is an internationally recognised framework for a best practice ISMS and compliance with it can be independently verified to both enhance an organization's image and give confidence to its customers.

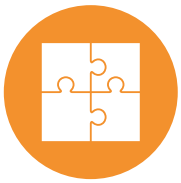
KEY PRINCIPLES AND TERMINOLOGY

The core purpose of an ISMS is to provide protection for sensitive or valuable information. **Sensitive information** typically includes information about employees, customers and suppliers. **Valuable information** may include intellectual property, financial data, legal records, commercial data and operational data.

THE TYPES OF RISKS THAT SENSITIVE AND VALUABLE INFORMATION ARE SUBJECT TO CAN GENERALLY BE GROUPED INTO THREE CATEGORIES:

Confidentiality

where one or more persons gain unauthorised access to information.



Integrity

where the content of the information is changed so that it is no longer accurate or complete.

Availability

where access to the information is lost or hampered.

These information security risk types are commonly referred to as "**CIA**".

Risks in information security typically arise due to the presence of **threats** and **vulnerabilities** to **assets** that process, store, hold, protect or control access to **information** which gives rise to **incidents**.

Assets in this context are typically people, equipment, systems or infrastructure.

Information is the data set(s) that an organization wants to protect such as employee records, customer records, financial records, design data, test data etc.

Incidents are unwanted events that result in a loss of **confidentiality** (e.g. a data breach), **integrity** (e.g. corruption of data) or **availability** (e.g. system failure).

Threats are what cause **incidents** to occur and may be malicious (e.g. a burglar), accidental (e.g. a key stroke error) or an act of God (e.g. a flood).

Vulnerabilities such as open office windows, source code errors, or the location of buildings next to rivers, increase the likelihood that the presence of a **threat** will result in an unwanted and costly **incident**.

In information security, risk is managed through the design, implementation and maintenance of **controls** such as locked windows, software testing or the siting of vulnerable equipment above ground floor levels.

An ISMS that complies with ISO 27001 has an interrelated set of best practice processes that facilitate and support the appropriate design, implementation and maintenance of **controls**. The processes that form part of an ISMS are usually a combination of existing core business processes (e.g. recruitment, induction, training, purchasing, product design, equipment maintenance, service delivery) and those specific to maintaining and improving information security (e.g. change management, information back-up, access control, incident management, information classification).

PDCA CYCLE

ISO 27001 is based on the Plan-Do-Check-Act (PDCA) cycle, also known as the Deming wheel or Shewhart cycle. The PDCA cycle can be applied not only to the management system as a whole, but also to each individual element to provide an ongoing focus on continuous improvement.

In brief:

Plan:

Establish objectives, resources required, customer and stakeholder requirements, organizational policies and identify risks and opportunities.

Do:

Implement what was planned.

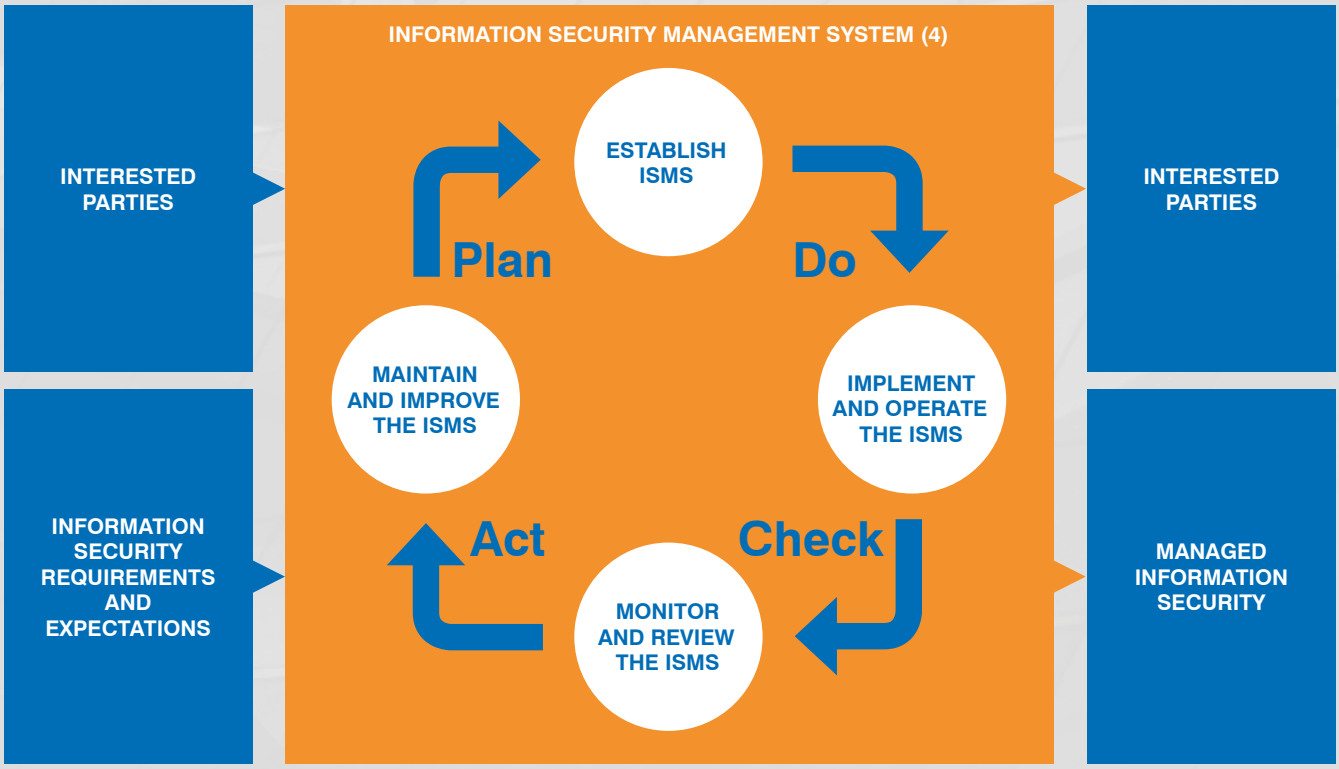
Check:

Monitor and measure processes to establish performance against policies, objectives, requirements and planned activities and report the results.

Act:

Take action to improve performance, as necessary.

PDCA model ISO 27001



Plan-Do-Check-Act is an example of a closed-loop system. This ensures the learning from the 'do' and 'check' stages are used to inform the 'act' and subsequent 'plan' stages. In theory this is cyclical, however it's more of an upward spiral as the learning moves you on each time you go through the process.

RISK BASED THINKING/AUDITS

Audits are a systematic, evidence-based, process approach to evaluation of your Information Security Management System. They are undertaken internally and externally to verify the effectiveness of the ISMS. Audits are a brilliant example of how risk-based thinking is adopted within Information Security Management.

1st Party Audits – Internal Audits

Internal audits are a great opportunity for learning within your organization. They provide time to focus on a particular process or department in order to truly assess its performance. The purpose of an internal audit is to ensure adherence to policies, procedures and processes as determined by you, the organization, and to confirm compliance with the requirements of ISO 27001.

Audit Planning

Devising an audit schedule can sound like a complicated exercise. Depending on the scale and complexity of your operations, you may schedule internal audits anywhere from every month to once a year. There's more detail on this in section 9 – performance evaluation.

Risk-based Thinking

The best way to consider frequency of audits is to look at the risks involved in the process or business area to be audited. Any process which is high risk, either because it has a high potential to go wrong or because the consequences would be severe if it did go wrong, should be audited more frequently than a low risk process.

How you assess risk is entirely up to you. ISO 27001 doesn't dictate any particular method of risk assessment or risk management.

2nd Party – External Audits

Second party audits are usually carried out by customers or by others on their behalf, or you may carry them out on your external providers. 2nd party audits can also be carried out by regulators or any other external party that has a formal interest in an organization.

You may have little control over the timing and frequency of these audits, however establishing your own ISMS will ensure you are well prepared for their arrival.

3rd Party – Certification Audits

Third party audits are carried out by external bodies, usually UKAS accredited certification bodies such as NQA.

The certification body will assess conformance to the ISO 27001:2013 standard. This involves a representative of the certification body visiting the organization and assessing the relevant system and its processes. Maintaining certification also involves periodic reassessments.

Certification demonstrates to customers that you have a commitment to quality.

CERTIFICATION ASSURES:

- regular assessment to continually monitor and improve processes.
- credibility that the system can achieve its intended outcomes.
- reduced risk and uncertainty and increase market opportunities.
- consistency in the outputs designed to meet stakeholder expectations.

PROCESS BASED THINKING/AUDIT

A process is the transformation of inputs to outputs, which takes place as a series of steps or activities which result in the planned objective(s). Often the output of one process becomes an input to another subsequent process. Very few processes operate in isolation from any other.

> ***"Process: set of interrelated or interacting activities that use inputs to deliver an intended result."***
>
> ISO 27001:2013 Fundamentals and Vocabulary

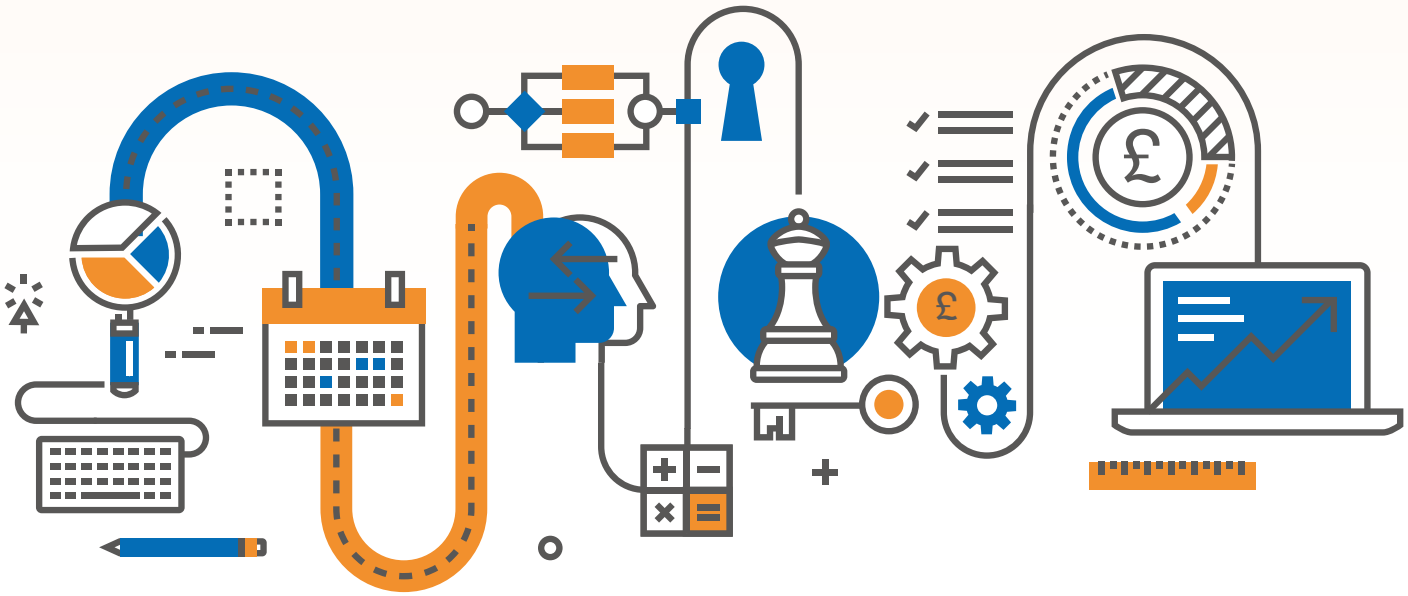
Even an audit has a process approach. It begins with identifying the scope and criteria, establishes a clear course of action to achieve the outcome and has a defined output (the audit report). Using the process approach to auditing also ensures the correct time and skills are allocated to the audit. This makes it an effective evaluation of the performance of the ISMS.

"Consistent and predictable results are achieved more effectively and efficiently when activities are understood and managed as interrelated processes that function as a coherent system."

ISO 27001:2013 Fundamentals and Vocabulary

Understanding how processes interrelate and produce results can help you to identify opportunities for improvement and thus optimise overall performance. This also applies where processes, or parts of processes, are outsourced. Understanding exactly how this affects or could affect the outcome and communicating this clearly to the business partner (providing the outsourced product or service) ensures clarity and accountability in the process.

The final process step is to review the outcome of the audit and ensure the information obtained is put to good use. A formal Management Review is the opportunity to reflect on the performance of the ISMS and to make decisions on how and where to improve. The Management Review process is covered in more depth in Section 9 – performance evaluation.

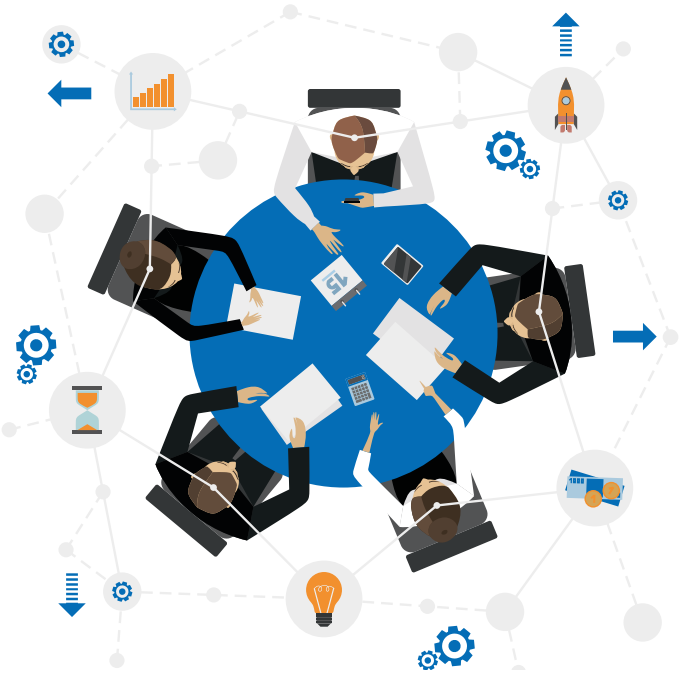


ANNEX SL

One of the major changes introduced into the 2013 revision of ISO 27001 was the adoption of Annex SL for the clause structure of the revised standard. Annex SL (previously known as ISO Guide 83) was used within ISO by standards writers to provide a common core structure for management system standards.

ISO 27001 (Information Security Management System Standard) adopted this structure during its 2013 revision. ISO 14001 (Environmental Management System Standard) also adopted this structure during its 2015 revision. The newly published ISO 45001 (Health and Safety Management System Standard) also follows this same common structure.

Prior to the adoption of Annex SL there were many differences between the clause structures, requirements and terms and definitions used across the various management system standards. This made it difficult for organizations to integrate the implementation and management of multiple standards; Environment, Quality, Health and Safety and Information Security being among the most common.



High Level Structure

Annex SL consists of 10 core clauses:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Of these clauses, the common terms and core definitions cannot be changed. Requirements may not be removed or altered, however discipline-specific requirements and recommendations may be added.

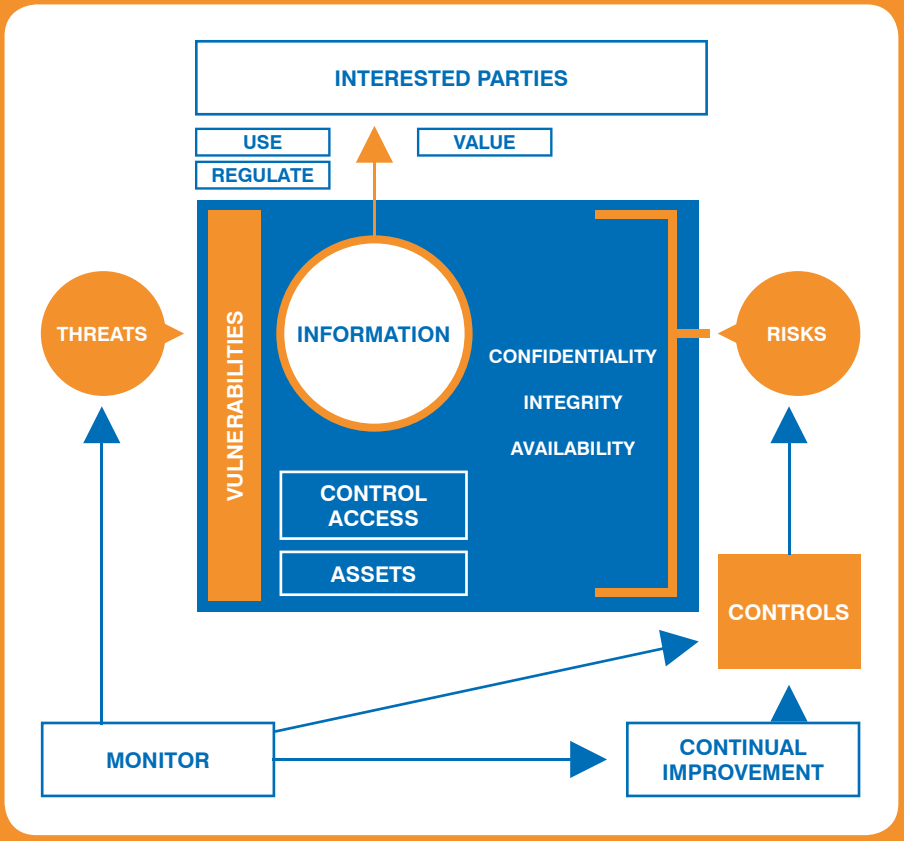
All management systems require a consideration of the context of the organization (more on this in section 4); a set of objectives relevant to the discipline, in this case quality, and aligned with the strategic direction of the organization; a documented policy to support the management system and its aims; internal audits and management review. Where multiple management systems are in place, many of these elements can be combined to address more than one standard.

THE 10 CLAUSES OF ISO 27001:2013

ISO 27001 is made of up 10 sections known as Clauses.

As with most other ISO management system standards, the requirements of ISO 27001 that need to be satisfied are specified in Clauses 4.0 – 10.0. Unlike most other ISO management system standards, an organization must comply with all of the requirements in Clauses 4.0 – 10.0; they cannot declare one or more clauses as being not applicable to them.

In ISO 27001, in addition to Clauses 4.0-10.0 there is a further set of requirements detailed in a section called Annex A, which is referenced in Clause 6.0. Annex A contains 114 best practice information security controls. Each of these 114 controls needs to be considered. To be compliant with ISO 27001 the organization must implement these controls, or an acceptable justification must be given for not implementing a particular control. The following parts of this guide provide an overview explanation of the purpose of each clause, highlight the type of evidence an auditor would expect to see to confirm that you comply, and give tips on effective ways to comply with the requirements.



CLAUSE 1: SCOPE

The Scope section of ISO 27001 sets out

- the purpose of the standard;
- the types of organizations it is designed to apply to; and
- the sections of the standard (called Clauses) that contain requirements that an organization needs to comply with in order for the organization to be certified as “conforming” to it (i.e. being compliant).

ISO 27001 is designed to be applicable to any type of organization. Regardless of size, complexity, industry sector, purpose or maturity, your organization can implement and maintain an ISMS that complies with ISO 27001.

CLAUSE 2: NORMATIVE REFERENCES

In ISO standards, the Normative References section lists any other standards that contain additional information that is relevant to determining whether or not an organization complies with the standard in question. In ISO 27001 only one document is listed – ISO 27000 Information Technology - Overview and vocabulary.

Some of the terms used or requirements detailed in ISO 27001 are explained further in ISO 27000. Reference to ISO 27000 is very useful in helping you to understand a requirement better or identify the best way to comply with it.

TIP – External auditors will expect you to have taken the information contained in ISO 27000 into account in the development and implementation of your ISMS.

CLAUSE 3: TERMS AND DEFINITIONS

There are no terms and definitions given in ISO 27001. Instead, reference is made to the most current version of ISO 27000 Information Security Management Systems – Overview and vocabulary. The current version of this document contains 81 definitions of terms that are used in ISO 27001.

In addition to the terms explained in the "Key Principles and Terminology" section above, the most important terms used in ISO 27001 are:

'Access Controls'

– processes that ensure that only the people that need to have access to a certain asset have that access and the "need" is determined with reference to both business and security requirements.

'Effectiveness'

– the extent to which planned activities (e.g. processes, procedures) are executed as planned or specified and achieve the planned results or outputs.

'Risk'

– a combination of the likelihood of an information security event occurring and the resulting consequences.

'Risk Assessment'

– the process of identifying risks, analysing the level of risk posed by each risk and evaluating whether additional action is needed to reduce each risk to a more tolerable or acceptable level.

'Risk Treatment'

– processes or actions that reduce identified risks to a tolerable or acceptable level.

'Top Management'

– the group of individuals who are the most senior decision makers in an organization. They are likely to be accountable for setting its strategic direction and for determining and achieving stakeholder objectives.

When you write your Information Security Management System documentation, you don't have to use these exact terms. However, it does help to clarify the meaning and intention if you can define the terms you have used. Providing a glossary within your system documentation may be useful.

CLAUSE 4: CONTEXT OF THE ORGANIZATION

The purpose of your ISMS is to protect your organization's Information Assets, so that the organization can achieve its goals.

How you go about this and the specific areas of priority will be driven by the context your organization operates in, both:

- **internal** – the things over which the organization has some control; and
- **external** – the things over which the organization has no direct control.

A careful analysis of the environment your organization operates in is fundamental to identifying the inherent risks posed to the security of your Information Assets. The analysis is the foundation that will enable you to assess what processes you need to consider adding or strengthening to build an effective ISMS.

Internal Context

The following are examples of the areas that can be considered when assessing the internal issues that may have a bearing on the ISMS risks:

- **Maturity:** are you an agile start-up with a blank canvas to work on, or a 30+ year old institution with well-established processes and security controls?
- **Organization culture:** is your organization relaxed about how, when and where people work, or extremely regimented? Might the culture resist the implementation of Information Security controls?
- **Management:** are there clear communication channels and processes from the organization's key decision makers through to the rest of the organization?
- **Resource size:** are you working with an Information Security Team, or is one person doing it all?
- **Resource maturity:** are the available resources (employees/ contractors) knowledgeable, fully trained, dependable and consistent, or are personnel inexperienced and constantly changing?
- **Information asset formats:** are your information assets mainly stored in hard-copy (paper) format, or are they stored electronically on a server on-site, or in remote cloud-based systems?
- **Information asset sensitivity/value:** does your organization have to manage highly valuable or particularly sensitive information assets?
- **Consistency:** do you have uniform processes in place across the organization, or a multitude of different operating practices with little consistency?
- **Systems:** does your organization have many legacy systems running on software versions that are no longer supported by the manufacturer, or do you maintain the most up to date and best available technology?
- **System complexity:** do you operate one main system that does all the heavy lifting, or multiple departmental systems with limited information transfer between them?
- **Physical space:** do you have a dedicated secure office facility, or do you operate in a space shared with other organizations?

External Context

The following are examples of the areas that can be considered when assessing the external issues that may have a bearing on the ISMS risks:

- **Competition:** do you operate in a rapidly changing and innovative market, requiring many system upgrades to stay competitive, or in a mature, stable market with little innovation year-to-year?
- **Landlord:** do you need approval to upgrade physical security?
- **Regulators / enforcement bodies:** is there a requirement in your sector to make regular statutory changes, or is there little oversight from regulators in your market sector?
- **Economic/political:** do currency fluctuations impact your organization; will Brexit in the UK have an impact?
- **Environmental considerations:** is your site on a flood plain with the server(s) located in a basement? Are there factors making your site(s) a possible target for a break-in or a terrorist attack (e.g. in a prominent city centre location; next to a possible target)?
- **Prevalence of information security attacks:** does your organization operate in a sector which regularly attracts interest from hackers (criminals, hacktivists)?
- **Shareholders:** are they very concerned about the vulnerability of the organization to data breaches? How concerned are they about the cost of the organization's efforts to improve its information security?

Interested Parties

An interested party is anyone who is, can be, or perceives themselves to be affected by an action or omission of your organization. Your interested parties will become clear through the process of carrying out a thorough analysis of internal and external issues. They will probably include shareholders, landlords, regulators, customers, employees and competitors and may extend to the general public and the environment, depending on the nature of your business. You don't have to try to understand or satisfy their every whim, but you do have to determine which of their needs and expectations are relevant to your ISMS.

Scope of the Management System

To comply with ISO 27001, you must document the scope of your ISMS. Documented scopes typically describe:

- the boundaries of the physical site or sites included (or not included);
- the boundaries of the physical and logical networks included (or not included);
- the internal and external employee groups included (or not included);
- the internal and external processes, activities or services included (or not included); and
- key interfaces at the boundaries of the scope.

If you want to prioritise resources by building an ISMS that doesn't cover all of your organization, selecting a scope that is limited to managing key stakeholder interests is a pragmatic approach. This can be done by including only specific sites, assets, processes and business units or departments. Some examples of scope statements:

- **"All operations carried out by the IT Department"**
- **"Support and management of email"**
- **"All equipment, systems, data and infrastructure in the organization's Data Centre based at the Basingstoke site"**

TIP – Document or maintain a file of all of the information collated in your analysis of your organization's context and interested parties such as:

- Discussions with a senior representative of the organization, e.g. an MD, CEO or CTO.
- Minutes of meetings or business plans.
- A specific document that identifies internal/external issues and interested parties and their needs and expectations e.g. a SWOT analysis, PESTLE study, or high-level business risk assessment.

CLAUSE 5: LEADERSHIP

The Importance of Leadership

Leadership in this context means active involvement in setting the direction of the ISMS, promoting its implementation and ensuring appropriate resources are made available. This includes:

- ensuring that the ISMS objectives are clear and aligned with overall strategy;
- that there is clarity on responsibilities and accountabilities;
- that risk-based thinking is at the heart of all decision making; and
- that there is clear communication of this information to all individuals within your ISMS scope.

ISO 27001 places great importance on active engagement by Top Management in the ISMS, based on the assumption that the engagement of Top Management is crucial in ensuring the effective implementation and maintenance of an effective ISMS by the wider employee group.

Information Security Policy

A vital responsibility of the leadership is to establish and document an Information Security Policy that is aligned with the key aims of the organization. At the top level it must either include objectives, or a framework (guidelines) for setting them. To demonstrate that it is aligned with your organization's context and the requirements of key stakeholders, it is recommended that it makes reference to, or contains a summary of, the principal issues and requirements it is designed to manage. It must also include a commitment to:

- satisfying applicable requirements relating to Information Security, such as legal requirements, customer expectations and contractual commitments; and
- the continual improvement of your ISMS.

The Information Security Policy may refer to, or include sub-policies that cover, the key controls of the organization's ISMS. Examples include: the selection of suppliers critical to Information Security, the recruitment and training of employees, clear desk and clear screen, cryptographic controls, access controls etc. To demonstrate the importance of the Information Security Policy, it is advisable that it is authorised by the most senior member of your Top Management or each member of the Top Management team.

TIP - To ensure your Information Security Policy is well communicated and available to interested parties, it is a good idea to:

- include it in induction packs and presentations for new employees and contractors;
- post the key statement on internal noticeboards, intranets and your organization's website; and
- make compliance with it and/or support for it a contractual requirement for employees, contractors and information security-critical suppliers.

Roles and Responsibilities

For Information Security activities to form part of the day-to-day activities for most people within the organization, the responsibilities and accountabilities they have must be defined and clearly communicated. Although there is no requirement in the standard for a nominated Information Security representative, it may be helpful for some organizations to appoint one to lead an information security team to coordinate training, monitoring controls and reporting on the performance of the ISMS to the Top Management. This individual may already hold responsibility for data protection or IT services. However, to carry out their role effectively they will ideally be a member of the Top Management team and either have a strong technical knowledge of information security management or access to individuals who do.

Evidencing Leadership to an Auditor

The Top Management will be the group of individuals who set the strategic direction and approve resource allocation for the organization or business area with your ISMS scope. Depending on how your organization is structured, these individuals may or not be the day-to-day management team. An auditor will typically test leadership by interviewing one or more members of your Top Management and assessing their level of involvement and participation in the:

- evaluation of risks and opportunities;
- establishment and communication of policies;
- setting and communication of objectives;
- review and communication of system performance; and
- allocation of appropriate resources, accountabilities and responsibilities.

TIP – Before your external audit, identify who from your Top Management will meet with the external auditor and prepare them for the interview with a dry run-through of the likely questions they will be asked.

CLAUSE 6: PLANNING

ISO 27001 is at heart a risk management tool that steers an organization to identify the drivers of its information security risks from the full range of sources. As such, the underlying purpose of an ISMS is to:

- **identify the strategically important, blatantly obvious, and hidden but dangerous risks;**
- **ensure that an organization's day-to-day activities and operating processes are designed, directed and resourced to inherently manage those risks; and**
- **automatically respond and adapt to changes to cope with new risks and continually reduce the organization's risk exposure.**

Having a detailed action plan that is aligned, updated and supported by regular reviews and monitoring is crucial, and provides the best evidence to the auditor of clearly defined system planning.

Risk Assessment

Risk assessment is at the core of any effective ISMS. Even the most well-resourced organization cannot completely eliminate the possibility of an information security incident occurring. For all organizations, risk assessment is essential to:

- increase the likelihood of identifying all potential risks through the involvement of key individuals using systematic assessment techniques;
- allocate resources to tackle the highest priority areas; and
- make strategic decisions on how to manage significant information security risks that will more likely realize their objectives.

Most risk assessment frameworks consist of a table containing the results of elements 1-4 with a supplementary table or matrix covering point 5.

An external auditor will expect to see a record of your risk assessment, an assigned owner for each risk identified and the criteria you have used.

TIP – Annex A (8.1.1) contains a requirement to maintain a list of information assets, assets associated with information (e.g. buildings, filing cabinets, laptops) and information processing facilities. If you complete your risk assessment by systematically assessing the risks posed to every item on this list, then you will have satisfied two requirements within the same exercise. Furthermore, for each item on the list, if you assign an owner you will also have satisfied another requirement in Annex A (8.1.2). As the asset owner is also likely to be the risk owner, this helps prevent duplication and potential confusion.

ISO 27005 – Information security risk management offers guidance on developing a risk assessment technique for your organization. Whichever technique you select or develop, it should include the following key elements:

1. Provide a prompt for systematic identification of risks (e.g. reviewing assets, groups of assets, processes, types of information) one at a time, checking each for the presence of common threats and vulnerabilities, and recording the controls you currently have in place to manage them.
2. Provide a framework for assessing the likelihood of each risk occurring on a consistent basis (e.g. once a month, once a year).
3. Provide a framework for assessing the consequences of each risk occurring on a consistent basis (e.g. £1,000 loss, £100,000 loss).
4. Provide a framework for scoring or categorizing each risk identified on a consistent basis (e.g. 1-10, high/medium/low), taking into account your assessment of the likelihood and consequences.
5. Set out documented criteria which specifies, for each risk score or category, what type of action needs to be taken and the level or priority assigned to it.

Risk Treatment

For each risk identified in your risk assessment, you must apply consistent criteria to determine whether you should:

- **accept the risk; or**
- **treat the risk (called "Risk Treatment")**

The Risk Treatment options available are normally one of the following:

- **Avoidance** – stop undertaking the activity or processing the information that is exposed to the risk.
- **Removal** – eliminate the source of the risk.
- **Change the likelihood** – implement a control that makes it less likely that an information security incident will occur.
- **Change the consequences** – implement a control that will lessen the impact if an incident occurs.
- **Transfer the risk** – outsource the activity or process to a third party that has greater capability to manage the risk.
- **Accept the risk** – if there is no practical risk treatment available to the organization, or the cost of the risk treatment is judged to be greater than the cost of the impact, you may make an informed decision to accept the risk. This would need to be approved by Top Management.

An external auditor will expect to see a Risk Treatment Plan (e.g. an action list) that details the risk treatment actions you have implemented or plan to implement. The plan must be sufficiently detailed to enable the implementation status of each action to be verified. There will also need to be evidence that this plan has been approved by the assigned risk owners and Top Management.

Annex A and the Statement of Applicability

All Risk Treatment options (with the exception of acceptance) involve the implementation of one or more controls. Annex A to ISO 27001 contains a list of 114 best practice information security controls. You will need to consider whether to implement each of these controls when formulating your Risk Treatment Plan. The description of most of the 114 controls is fairly vague, so it is strongly recommended that you review ISO 27002 which contains more information on best practice ways of implementing them.

As evidence of you having completed this assessment, an external auditor will expect you to produce a document called a Statement of Applicability. Within this, for each of the 114 controls you must record:

- whether it is applicable to your activities, processes and information security risks;
- whether you have implemented it or not; and
- if you have deemed it not applicable, your justification for doing so.

For most organizations, the majority of the 114 controls will be applicable, and they are likely to have already implemented a number of them to some degree.

TIP - Your Statement of Applicability does not need to an overly complex document. A simple table with column headings Control, Applicable?, Implemented?, and Justification will suffice. It is also advisable to record some information on how the control has been applied (e.g. reference a procedure or policy) to help you more readily answer any questioning from your external auditor.

Information Security Objectives and Planning to Achieve Them

At relevant levels within your organization you need to have a documented set of information security-related objectives. These can be at a top level and apply organization-wide (e.g. "achieve ISO 27001 certification") or departmental (e.g. "complete Information Security Briefings for all new starters within 1 week of their start date").

Each objective you set must:

- be measurable;
- be aligned with your Information Security Policy;
- take account of the organization's information security requirements; and
- take account of the output from the risk assessment and risk treatment process.

Typical objectives that are relevant to information security include:

- Not exceeding a defined frequency of certain types of information security incidents.
- Achieving a measurable level of compliance with information security controls.
- Providing a defined availability of information services.
- Not exceeding a measurable number of data errors.
- Making improvements to available resources through recruitment, training or acquisition.
- Implementation of new controls.
- Achieving compliance with information security-related standards.

Each objective must be communicated to relevant persons. The objectives must be updated when necessary to keep them relevant and to assess performance against them.

For each of the objectives you need to plan how you are going to achieve them. This includes determining:

- what needs to be achieved;
- what resources are assigned;
- who has ownership or primary responsibility for delivering against the objective;
- whether there is a target date for completion or just an ongoing requirement; and
- the method of assessing performance against the objective (i.e. what is your measure).

TIP - Effective ways to communicate Information Security Objectives include covering them in induction training, setting them as employee objectives or including them in employee appraisals, establishing them in SLAs with suppliers, or evaluating performance against them in supplier performance reviews.

CLAUSE 7: SUPPORT

Clause 7 concerns itself with resources. This applies to people, infrastructure and environment as much as physical resources, materials, tools etc. There is also a renewed focus on knowledge as a significant resource within your organization. When planning your quality objectives, a major consideration will be the current capacity and capability of your resources as well as those you may need to source from external suppliers / partners.

To implement and maintain an effective ISMS you need to have supporting resources in place. These resources will need to be sufficiently:

- **capable** – if they are equipment or infrastructure; and
- **competent** – if they are people.
- at Management Review meetings.

Competence

The implementation of effective information security controls relies heavily on the knowledge and skills of your employees, suppliers and contractors. To be certain of an appropriate knowledge and skills base you need to:

- define what knowledge and skills are required;
- determine who needs to have the knowledge and skills; and
- set out how you can assess or verify that the right people have the right knowledge and skills.

Your auditor will expect you to have documents detailing your knowledge and skills requirements. Where you believe the requirements are satisfied this will need to be supported with records such as training certificates, course attendance records or internal competency assessments.

TIP – Most organizations that already use tools such as training/skills matrices, appraisals or supplier assessments can satisfy the requirement for competence records by expanding the areas covered to include information security.

Awareness

In addition to ensuring specific competence of key personnel in relation to information security, the wider group of employees, suppliers and contractors will need to be aware of the basic elements of your ISMS. This is central to establishing a supportive culture within the organization.

All staff, suppliers and contractors should be aware of the following:

- That you have an ISMS and why you have one.
- That you have an Information Security Policy and which particular elements of it are relevant to them.
- How they can contribute to your organization protecting its valuable information and what they need to do to help the organization achieve its information security objectives.
- Which policies, procedures and controls are relevant to them and what the consequences are of not complying with them.

TIP – The communication of this information can normally be done through existing processes and documents such as inductions, employment contracts, toolbox talks, supplier agreements, employee briefings or updates.

Communication

To enable the processes in your ISMS to work effectively you will need to ensure you have communication activities that are well planned and managed. ISO 27001 details these concisely by requiring you to determine:

- what needs to be communicated;
- when it needs to be communicated;
- to whom it needs be communicated;
- who is responsible for communication; and
- what is the processes for communication.

TIP – If your communication requirements are well defined in your processes, policies and procedures then you do not need to do any more to satisfy this requirement. If they aren't then you should consider documenting your key communication activities in the form of a table or procedure that includes the headings detailed above. Remember, the content of these documents also needs to be communicated!

Documented Information

To be of use, the documented information you use to implement and maintain your ISMS needs to:

- be accurate;
- be understandable to the individuals who use it regularly or occasionally; and
- support you to comply with legal requirements, manage information security risks and achieve your objectives.

So that your documented information always satisfies these requirements you will need to have processes in place to ensure that:

- documented information is reviewed where required by appropriate individuals before it is released into general circulation;
- access to documented information is controlled so that it cannot be changed accidentally, corrupted, deleted or accessed by individuals to whom it is not appropriate;
- information is deleted securely or returned to its owner when there this a requirement to do this; and
- you can track changes to information to guarantee that the process is in control.

The source of your documented information may be either internal or external, so your control processes need to manage documented information from both sources.

TIP – Organizations that have good document control typically have one or more of the following in place:

- A single person or small team responsible for ensuring that new/modified documents are reviewed before they are issued, are stored in the right location, are withdrawn from circulation when superseded and that a register of changes is maintained.
- An electronic document management system that contains automatic workflows and controls.
- Robust electronic data back-up and hard-copy file archiving/storage processes.
- Strong employee awareness of document control, record keeping and information access/retention requirements.

CLAUSE 8: OPERATION

So, after all the planning and risk assessment, we're ready to move on to the "do" stage. Clause 8 is all about having appropriate control over the creation and delivery your product or service.

Managing your information security risks and achieving your objectives requires the formalisation of your activities into a set of clear and coherent processes.

Many of these processes are likely to exist already (e.g. induction, training) and will simply need modifying to include elements relevant to information security. Other processes may happen in an ad-hoc fashion (e.g. supplier approvals), while some may not currently exist at all (e.g. internal audit).

To implement effective processes the following practices are crucial:

1. Processes are created by adapting or formalising an organization's "business as usual" activities.
2. Systematic identification of the information security risks relevant to each process.
3. Clear definition and communication of the set of activities required to manage the associated information security risks when an event occurs (e.g. a new employee joining the company).
4. Clear assignment of the responsibilities for carrying out related activities.
5. Adequate allocation of resources to ensure that related activities can take place as and when required.
6. Routine assessment of the consistency with which each process is followed and its effectiveness in managing relevant information security risks.

TIP – For each process, designate an individual as accountable for ensuring that steps 2-6 happen. This individual is often referred to as the Process Owner.

Information Security Risk Assessment

The risk assessment methods and techniques described in Clause 6 must be applied to all processes, assets, information and activities within the organization's ISMS scope.

Since risks are not static, the results of these assessments must be reviewed at appropriate frequencies. This is usually at least annually, or more frequently if the assessment identifies the presence of one or more significant risks. Risks should also be reviewed whenever:

- any Risk Treatment actions are completed (see below);
- there are changes to the organization's assets, information or processes;
- new risks are identified; or
- experience or new information indicates that the likelihood and consequence of any identified risk has changed.

TIP – To ensure your risk assessment process covers the types of events that would require a review, you should also take into consideration the Annex A controls for Technical Vulnerability Management (A.12.6), Security in Development and Support Processes (A.14.2) and Supplier Service Delivery Management (A.15.2).

Information Security Risk Treatment

The risk treatment plan you develop cannot simply remain as a statement of intent; it must be implemented. Where changes are needed to take into account new information about risks and changes to your risk assessment criteria, the plan needs to be updated and re-authorised.

The impact of the plan must also be assessed and the results of this assessment recorded. This may be done as part of your Management Review or Internal Audit Processes or by using technical assessments such as network penetration tests, supplier audits or unannounced third part audits.

CLAUSE 9: PERFORMANCE EVALUATION

There are three main ways in which the performance of an ISMS is evaluated. These are:

- monitoring the effectiveness of the ISMS controls;
- through internal audits; and
- at Management Review meetings.

Monitoring, Measurement, Analysis and Evaluation

Your organization will need to decide what needs to be monitored to be assured that your ISMS process and information security controls are operating as intended. It is impractical for an organization to monitor everything all the time; if you attempt to do so, it is likely that the volume of data would be so great that it would be virtually impossible to use it effectively. Therefore, in practice, you will need to take an informed decision about what to monitor. The following considerations will be important:

- Which processes and activities are subject to the most frequent and significant threats?
- Which processes and activities have the most significantly inherent vulnerabilities?
- What is practical to monitor and generate meaningful and timely information from?
- With each monitoring process you put in place, for it to be effective you must clearly define:
- how the monitoring is undertaken (e.g. is this defined in a procedure);
- when it is undertaken;
- who is responsible for undertaking it;
- how are the results reported, when, to whom and what do they do with them; and
- if the monitoring results identify unacceptable performance, what is the escalation process or procedure to deal with this situation.

To demonstrate to an auditor that you have appropriate monitoring processing in place, you will need to retain records of monitoring results, analysis, evaluation reviews and any escalation activities.

Internal Audits

The purpose of internal audits is to test your ISMS processes for weaknesses and identify opportunities for improvement. They are also an opportunity to provide a reality check to Top Management on how strongly the ISMS is performing. When done well, internal audits can ensure that there are no surprises at your external audits.

The internal audits you perform should check:

- how consistently processes, procedures and controls are followed and applied;
- how successful your processes, procedures and controls are at generating the intended results; and
- whether your ISMS remains compliant with ISO 27001 and the requirements of interested parties.

To ensure that audits are undertaken to a high standard and in a way that is seen to add value, they need to be undertaken by individuals who:

- are respected;
- competent
- understand the requirements of ISO 27001; and
- can quickly interpret your documentation and are well-practiced in sound auditing techniques and behaviours.

Most importantly of all, they need to be allocated sufficient time to do the audit and be assured of cooperation from relevant employees. You must maintain a plan for carrying out your internal audits. An external auditor will expect this plan to ensure that all of your ISMS processes are audited over a three-year cycle and that processes which:

- have shown evidence of poor performance (i.e. through previous audits, or monitoring results or information security incidents); and/or
- manage the most significant information security risks
- are audited at a higher frequency.

The external auditor will also expect that any actions identified from audits are recorded, reviewed by appropriate employees and actions implemented in a timely manner to rectify any significant issues. They should make an allowance in the close-out time for any improvement opportunities identified that require significant investment in resources.

Management Review

Management Review is an essential element of an ISMS. It is the formal point at which Top Management reviews the effectiveness of the ISMS and ensures its alignment to the organization's strategic direction. Management Reviews must take place at planned intervals and the overall review programme (i.e. one meeting or several meetings) must at a minimum cover a list of core areas specified within clause 9.3 of the standard.

It is not essential for one single Management Review meeting to take place covering the full agenda. If you currently hold a range of meetings that cover the inputs between them, there is no specific need to duplicate them.

You will need to retain documented information on your Management Reviews. These would normally be minutes of meetings or perhaps call recordings if you carry out conference calls. These do not need to be extensive notes, but they must contain a record of any decisions made and actions agreed, ideally with responsibilities and timescales.

TIP – If you decide to adapt your existing schedule of management meetings and these meetings cover a number of areas, you may want to consider summarising the areas that these meetings cover in the form of a table or procedure so that it is clear to you and an auditor which meetings cover each of the required review areas.

CLAUSE 10: IMPROVEMENT

The key aim of implementing an ISMS should be to reduce the likelihood of information security events occurring and their impact. No ISMS is likely to be perfect. However, a successful ISMS will improve over time and increase the organization's resilience to information security attacks.

Nonconformity and Corrective Action

One of the main drivers of improvement is to learn from security incidents, issues identified in audits, performance issues identified from monitoring, complaints from interested parties and ideas generated at management reviews.

For each learning opportunity identified you must maintain a record of:

- what occurred;
- if the event had undesirable consequences, what action was taken to contain and mitigate those;
- the root cause of the event (if determined);
- the action taken to eliminate the root cause (if needed); and
- an assessment of the effectiveness of any action taken.

Root cause analysis

To identify effective corrective action, it is strongly advisable to complete a root cause analysis of the issue that occurred. If you don't get to the bottom of why or how it happened, then it is likely that whatever fix you implement will not be fully effective. A simple approach such as "5 Whys" is a good root cause analysis tool: start with the issue, then ask "Why" enough times to reach the root cause. Usually 5 times of asking is enough, but for more complex problems you may need to dig deeper.

For example:

Problem statement:

The organization was infected by the Wannacry virus

Why?

Someone clicked on a link in an email and it downloaded the virus and infected their PC

Why?

They had not received any training in clicking on links in emails they are not expecting to receive

Why?

The training manager is on maternity leave and the organization has not implemented cover for them

Why?

The maternity leave process is not covered in the Change Management Procedure and so a risk assessment was not completed to identify any information security risks.

TIP – You may not have sufficient resources to undertake root cause analysis for every event. To prioritise your efforts, you should consider first completing a simple risk assessment of an event and then undertake root cause analysis only for those that are medium or high risk.

GET THE MOST FROM YOUR MANAGEMENT SYSTEMS

Top Tips for the successful implementation of an ISMS

1. Start with “Why?”. Make sure the reasons for implementing an ISMS are clear and aligned with your strategic direction, otherwise you risk not getting the critical buy-in from Top Management.

2. Next consider “What for?”. Implementing and maintaining an ISMS requires significant commitment, so make sure your scope is broad enough to cover the critical information that needs protecting, but is not so broad that you do not have sufficient resources to implement and maintain it.

3. Get all of your key stakeholders involved at the appropriate times. Top Management for context, requirements, policy and objectives setting; managers and employees with valuable knowledge for risk assessments, process design and procedure writing.

4. Communicate extensively throughout the process to all of your stakeholders. Let them know what you are doing, why you’re are doing it, how you plan to do it and what their involvement will be. Provide regular progress updates.

5. Get external help where you need it. Do not fail for lack of in-house technical skills or knowledge. Management of information security risks often requires specialist knowledge. However, be sure to check the credentials of a third party before engaging them.

6. Keep your processes and supporting documentation simple. It can develop to become more extensive over time if needed.

7. Design and implement rules you can follow in practice. Don’t make the mistake of documenting an over-elaborate rule that no-one can follow. It is better to accept a risk and to continue to look for ways to manage it.

8. Remember your suppliers. Some suppliers will help you enhance your ISMS, some will increase your risk. You need to ensure any high-risk suppliers have controls in place that are at least as good as yours. If they don’t then look for alternatives.

9. Train, train and train again. Information Security is likely to be a new concept for many or most of your employees. People may need to change habits ingrained over many years. A single awareness briefing is unlikely to be sufficient.

10. Remember to allocate sufficient resources to routinely test your controls. The threats your organization faces will constantly change and you need to test whether you are able to respond to those threats.

NEXT STEPS ONCE IMPLEMENTED

1 AWARENESS TRAINING

- Your organization should raise awareness about various standards covered under IMS.
- You should hold separate training meetings for top management, middle management and junior level management, which will help to create a motivating environment, ready for implementation.

2 POLICY AND OBJECTIVES

- Your organization should develop an Integrated Quality Policy/Environment Policy/Health & Safety Policy/Information Security Policy and relevant objectives to help meet the requirements.
- By working with top level management your company should hold workshops with all levels of management staff to outline the integrated objectives.

3 INTERNAL GAP ANALYSIS

- Your organization should identify and compare the level of compliance of existing systems against requirements of the standards under your new IMS.
- Relevant staff should all understand the operations of the organization and develop a process map for the activities within the business.

4 DOCUMENTATION / PROCESS DESIGN

- The organization should create documentation of the processes as per requirements of relevant standard(s).
- You should write and implement a manual, functional procedures booklet, work instructions, system procedures and provide associated terms.

5 DOCUMENTATION / PROCESS IMPLEMENTATION

- Processes / Documents developed in step 4, should be implemented across the organization covering all the departments and activities.
- The organization should hold a workshop on the implementation as per applicable for the ISO standard requirements.

6 INTERNAL AUDIT

- A robust internal audit system for the organization is essential. Internal Auditor Training is recommended and NQA can provide Internal Auditor Training for the standard(s) that you are implementing.
- It is important to implement corrective actions for improvements, in each of the audited documents, in order to bridge gaps and ensure effectiveness of IMS.

7 ORGANISE A MANAGEMENT 'SYSTEM' REVIEW MEETING

- Top level management must review various official business aspects of the organization, which are relevant to the standards being implemented.
- Review the policy, objectives, results of internal audit, results of process performance, results of complaints/feedback/legal compliance, results of risk assessment/incidents and develop an action plan following the meeting - which must be minuted.

8 THOROUGH GAP ANALYSIS OF IMPLEMENTED SYSTEMS

- A formal pre-certification gap analysis should be conducted to assess effectiveness and compliance of system implementation in the organization.
- This final gap analysis will prepare your organization for the final certification audit.

9 CORRECTIVE ACTIONS

- The organization should be ready for final certification audit, providing that the gap analysis audit conducted in the last step and all the non-conformities (NC) have been assigned corrective actions.
- Check that all the significant NCs are closed and the organization is ready for the final certification audit.

10 FINAL CERTIFICATION AUDIT

- Once completed, your organization is hopefully recommended for registration to the required standard.
- CONGRATULATIONS!

NOTES

NOTES

Authored on behalf of NQA by: Julian Russell

nqa.
www.nqa.com