ISO 27001 Information Security Management System 10-Step Guide

CONTENTS

INTRODUCTION

ISO 27001 Certification

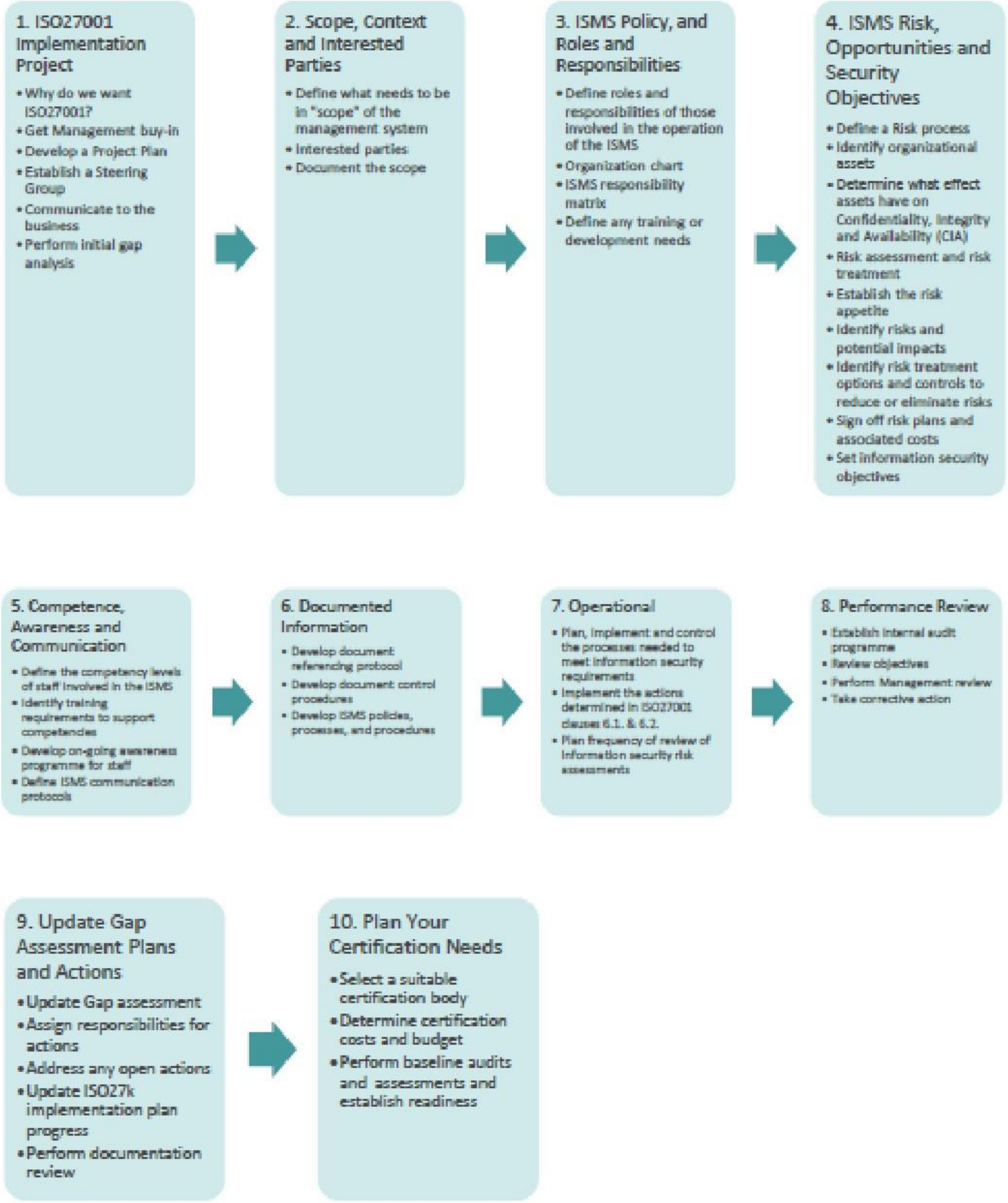
The ISO27001 standard is recognized worldwide as one of the foremost information security frameworks. Adopted by organizations small and large across a wide variety of industries, certification to ISO27001 is increasingly seen as a de facto requirement in competitive tendering situations, and as an assurance to stakeholders that cyber security is taken seriously.

We often come across the situation where one of our customers has decided that they need to become certified to the ISO27001 standard, but they're not sure how to go about it.

Sometimes, their customers have told them that it is a requirement. So, to carry on doing business, it's a must.

This guide takes you through the journey to ISO27001 certification and sets out the main steps along the way. Note this guide can be used whether certifying to the 2013/17 or 2022 version of the standard.

THE CERTIFICATION JOURNEY



1. ISO27001 Implementation Project
- Why do we want ISO27001?
- Get Management buy-in
- Develop a Project Plan
- Establish a Steering Group
- Communicate to the business
- Perform initial gap analysis

2. Scope, Context and Interested Parties
- Define what needs to be in "scope" of the management system
- Interested parties
- Document the scope

3. ISMS Policy, and Roles and Responsibilities
- Define roles and responsibilities of those involved in the operation of the ISMS
- Organization chart
- ISMS responsibility matrix
- Define any training or development needs

4. ISMS Risk, Opportunities and Security Objectives
- Define a Risk process
- Identify organizational assets
- Determine what effect assets have on Confidentiality, Integrity and Availability (CIA)
- Risk assessment and risk treatment
- Establish the risk appetite
- Identify risks and potential impacts
- Identify risk treatment options and controls to reduce or eliminate risks
- Sign off risk plans and associated costs
- Set information security objectives

5. Competence, Awareness and Communication
- Define the competency levels of staff involved in the ISMS
- Identify training requirements to support competencies
- Develop on-going awareness programme for staff
- Define ISMS communication protocols

6. Documented Information
- Develop document referencing protocol
- Develop document control procedures
- Develop ISMS policies, processes, and procedures

7. Operational
- Plan, Implement and control the processes needed to meet information security requirements
- Implement the actions determined in ISO27001 clauses 6.1. & 6.2.
- Plan frequency of review of information security risk assessments

8. Performance Review
- Establish internal audit programme
- Review objectives
- Perform Management review
- Take corrective action

9. Update Gap Assessment Plans and Actions
- Update Gap assessment
- Assign responsibilities for actions
- Address any open actions
- Update ISO27k implementation plan progress
- Perform documentation review

10. Plan Your Certification Needs
- Select a suitable certification body
- Determine certification costs and budget
- Perform baseline audits and assessments and establish readiness

Figure 1 The certification journey to Stage 1

STEP ONE

PROJECT IMPLEMENTATION

WHY GET CERTIFIED?

Certification to any management system standard requires effort and resources, not only to set up and establish the system and its associated policies and core activities, but the longer-term aspects of operating and maintaining it. An essential first question is: “Why do we want to formally certify to the ISO27001 standard?”

INTERNALLY DRIVEN NEED

You may have an internally driven need:

- To be more efficient or improve ways of working
- To reduce business risks
- Reduce defects or incidents that impact business reputation
- To provide internal recognition

EXTERNALLY DRIVEN NEED

Or perhaps an externally driven need:

Customer requirement: Contractual requirements are often a main reason you may be considering certifying to an ISO standard. Even so, if you embrace the requirements in the standard appropriately, your business should gain many of the benefits indicated above.

Cyber-crime: Your company may have become a target. As unfortunate as this is, cyber- crime is increasing, so it is more important than ever to protect the data security of your customers and employees. Cyber criminals are becoming more sophisticated, with regular reports of high-profile organizations being attacked. Is your organization keeping confidential and personal data safe?

It is still possible to align your business processes and operations to the standard without going the extra step of certification - you just don’t open your organization up for audit or scrutiny on a periodic basis with a certification body. The downside to this is that you cannot claim or demonstrate to customers that you are indeed compliant during bidding or tendering opportunities.

GET MANAGEMENT BUY-IN

The first step, and undoubtedly one of the most important, is to ensure you have the commitment from top management. If those in charge of the budgets and business direction don't think your information security system (ISMS) is a good idea, it is going to founder at some point, no matter how much effort you put into it. Make sure they're on board.

"If those in charge don't think your ISMS is a good idea, it is going to flounder."

DEVELOP A PROJECT PLAN

No mature organization would enter development of its product or services without a plan. Similarly, the implementation of an ISMS requires a plan to ensure that everyone involved knows what tasks they are responsible for and when those tasks need to be completed.

Responsibility should be assigned by the CEO/Executive Sponsor to an individual to plan and co-ordinate the ISO27001 implementation activities.

ESTABLISH A STEERING GROUP

The size and extent of a steering group will be very much dependent on the size of your organization and the roles directly impacted by the ISMS. Aim to set up a series of regular group meetings to review progress against the implementation plan.

Involve representatives from across the business who are responsible and accountable for decisions that involve:

- Establishing policy and processes, ISMS objectives and plans
- Budgets
- Risks and treatment decisions
- Assignment of tasks

The steering group should also have an executive sponsor responsible for the above, the operation of the ISMS within the organization, and for delegation of authority where appropriate.

COMMUNICATION IS KEY

When you embark on the journey to certification, it is important to brief staff across the business on two key things:

- Why you want to achieve certification to ISO27001, and what are the drivers for it
- That senior management endorses the plan and is committed to achieving certification

PERFORMING AN INITIAL GAP ASSESSMENT

By performing a gap assessment, you will gain a better appreciation of how much work may be involved in getting to a point where a certification audit is possible.

The key to conducting an accurate gap assessment is to get the right people involved so that you have a full understanding of what is already in place. Tools like the ISO27001 Gap Assessment in the CertiKit toolkit will provide hard figures on how compliant you currently are by area of the standard and will even show you the position on bar charts to share with top management.

It is a good idea to repeat the exercise on a regular basis during your project to assess your level of progress from the original starting point.

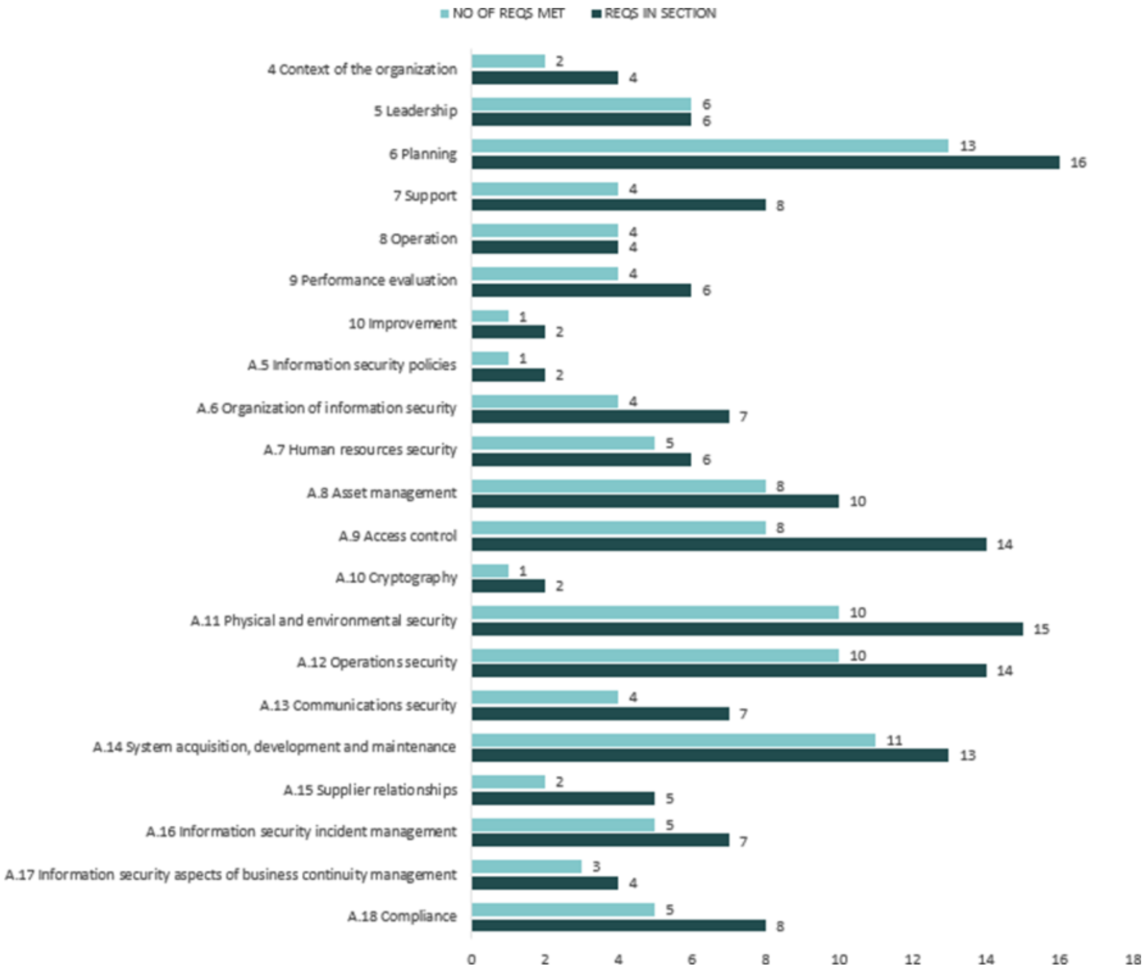


Figure 2 Chart showing the level of conformity to the standard in the ISO27001 toolkit's Gap Assessment tool (ISO27001:2013 version)

STEP TWO

SCOPE, CONTEXT AND INTERESTED PARTIES

DEFINE YOUR ISMS SCOPE

You don't have to have everything within the scope of your management system, so a necessary early step is to draw a ring around what's included and be able to justify what's not. You must get this right because every step from here is affected by it, so take your time. Also required is to set out what the standard calls the "context" of your management system – this is really the environment that your organization operates within, both outside and inside its boundaries.

INTERESTED PARTIES

The ISO27001 standard requires you to define all the interested parties who are "relevant" to the management system. So, who are these interested parties? As a starting point the key interested parties for most organizations will typically include:

- Your customer(s): Customers may contractually require you to deliver products and services that comply with specific requirements
- Legal and regulatory bodies: Local, regional or national rules that apply to you as a business. These often have a direct impact on your management system as you will likely have to implement procedures and controls to address these requirements.
- Suppliers: ISO27001 has several requirements addressing supplier relationships regarding information security. In particular, managing risks associated with suppliers' access to any of your organizations assets such as systems, or even physical access to premises etc.

You should allow time to develop an understanding of your business's internal and external stakeholder interests that might impact upon your management system's ability to deliver its intended results. What this means is that you must understand what influence they have, then figure out what you need to do to address these interests through ISMS policy, procedure, controls, or other means. Also, interested party requirements could introduce risks that you have to recognize and mitigate.

DOCUMENT THE SCOPE

The Registered Certification Body (RCB) who will perform your certification assessment at some stage will need to know the boundaries of your management system. Having a documented scope helps you convey to the RCB where your ISMS starts and ends.

STEP THREE

POLICY, ROLES AND RESPONSIBILITIES

ROLES AND RESPONSIBILITIES

There will be several key roles that will be required for the effective operation of the ISMS. The following list is not set in stone and will very much depend on the size and scope of the ISMS itself. Some of these roles may be combined and responsibilities shared accordingly:

- Information security steering group - (see step 1)
- Information security manager - often also called the Chief Information Security Officer (CISO) is the primary role with a dedicated focus on information security and related issues.
- Information asset owner - has primary operational responsibility for one or more information assets as defined in the organization's Information Asset Inventory.
- Information security risk owner - has primary responsibility for managing one or more information security risks as defined in the organization's Risk Treatment Plan.
- Information security auditor - fulfils the internal audit requirements of the ISO/IEC 27001 standard and is generally responsible for checking that the ISMS is effectively implemented and maintained.
- Other roles with information security responsibilities such as:
    - Department managers
    - IT technicians
    - IT users

ORGANIZATION CHART

It is important to develop an organization chart showing the reporting lines and relationships of all those involved in the operation of the ISMS.

ISMS RESPONSIBILITY MATRIX

One useful approach for showing responsibility for the management of the various sections of the ISO27001 standard is to use a RACI table. This defines the type of responsibility of each role in each area according to whether the listed role is responsible, accountable, consulted or informed.

STEP FOUR

RISK, OPPORTUNITIES AND SECURITY

DEFINE A RISK PROCESS

Before you begin the risk assessments, you need to define the risk process you want to apply within the organization. There are many methods and approaches to performing risk assessments, so it is important to select one that is suitable for your needs and is not over complicated. More importantly the approach you select needs to help you identify as efficiently as possible the risks and their impacts, and what actions to take.

Some things to consider:

- Do you want to apply a particular approach or method? Such as:
  - Qualitative Risk Assessment - this tends to be subjective. It focuses on identifying risks and assessing the likelihood and impact of a specific risk event on a numerical scale, for example 1-5.
  - Quantitative Risk Assessment - this uses verifiable data to analyse the effects of risk, for example, RISK A has a 40% chance of occurring, based on quantifiable data, RISK B has a 20% chance of occurring based on the same input data.
  - Generic Risk Assessment - this highlight commonly identified hazards (for instance, things with the potential to cause harm) and control measures/precautions. This approach is typically used in Health and Safety risk assessments but does have relevance to Information Security if you consider risks in the same way as potential to cause harm or damage to your business and its systems.
- What risk templates and documentation are required to support the approach you select?
- What skills and competency do you have to perform an effective risk assessment?

ORGANIZATIONAL ASSETS

This is another important part of the ISO27001 standard and is key to addressing several questions:

- What assets does the organization have, so that they can be suitably protected from accidental loss, theft, or malicious attack. Additionally, when staff leave the business, it is important to ensure the return of company assets that have been assigned to that individual.

- What information assets does the organization have that are critical to control in terms of impact on information security, and what aspects of information security do they have the biggest effect upon.

When staff leave the business, it is important to ensure the return of company assets

ASSETS’ EFFECTS ON CIA

For each asset, determine if the loss would impact the Confidentiality, Integrity, or Availability (CIA) of the information processed or contained on that asset. Determining CIA helps you assess the nature of the risks to the business.

RISK APPETITE

This is a key decision to make as it will ultimately determine how you approach and deal with risks that you identify. For example, if you are risk averse then you may want to act and treat most risks that you identify in your risk assessment. Alternatively, if you are not too cautious about risk then you may be prepared to accept or defer actions for risks identified.

RISKS AND IMPACTS

Now we come to one of the key foundations of an ISO27001 management system – risk assessment and treatment. This involves identifying actions you need to take to protect your assets from various threats that are out there (and within your own organization of course).

These actions are often referred to as ‘controls' and the ISO27001 standard provides a full set of reference controls within Annex A. One of the key documents from an audit viewpoint is the Statement of Applicability which sets out which of these reference controls you feel are applicable to your organization.

RISK TREATMENT

Now that you have all your risks documented and scored, the next step is to select the most appropriate controls from the Annex A control set that will mitigate or reduce the risks identified. The risk appetite may also determine which treatment options you choose and which to prioritise first.

SIGN OFF RISK PLANS

You may need to demonstrate the outputs of the risk process and treatment decisions to the leadership team for approval and funding. This is typically done by consolidating the higher risk items and documenting them in a risk treatment plan for acceptance.

INFOSEC OBJECTIVES

The establishment of information security objectives is key to driving the implementation of ISO27001 in a particular direction. Typically, at the start of implementing an ISMS, many of the objectives will be based on achieving certification as well as the other key drivers to achieving a successful outcome. However, the objectives should be a living and actively maintained list that changes over time.

In terms of the ISMS there are two main levels of objectives. The first is the high-level objectives set out when defining the context of the ISMS. The second level of objectives is more action-oriented and will refer to a fixed timeframe. Typically, these will be specific objectives that are planned in a particular financial year, are time dependent due to stakeholder needs, or could be security incidents or improvements that need to be addressed in a certain time.

STEP FIVE

COMPETENCE AND AWARENESS

STAFF COMPETENCE LEVELS

Ensure that the roles and responsibilities, as described in a previous step, are documented within the ISMS and that the competencies and role requirements are defined and documented for each.

TRAINING AND DEVELOPMENT

The standard simply requires that adequate resources are provided for the ISMS to function effectively, which means that senior management will have to consider what existing resources you have internally to fulfil the roles required to support the ISMS and whether you have resource gaps that will need to be filled.

Some roles will require training in understanding the ISO27001 requirements and their interpretation, whereas others need just a general awareness of policies and procedures that they must comply with.

ONGOING AWARENESS

Ensure staff are regularly updated on the ISMS development programme and its outputs. More importantly, give awareness training on key information security topics that apply to users in the business. This could include policies, risks, security controls, general awareness, and induction training.

COMMUNICATION PROTOCOLS

Define a communications plan that shows all the methods of communication, who is responsible for each, and how things will be communicated.

STEP SIX

DOCUMENTED INFORMATION

DOCUMENT REFERENCING

All ISMS documents like policies, processes, procedures, templates and forms need some unique way of numbering to identify them.

DOCUMENT CONTROL

The proper control of your ISMS policies, procedures and documents is a key requirement of any management system standard. You should ensure that you have a defined and documented set of document control procedures that cover the lifecycle of documented information.

Consideration should also be given to records, and their lifecycle should be determined along with defined methods for identification, storage, protection, retrieval, retention and disposal.

The proper control of documents is a key requirement of any information security management system

POLICIES AND PROCEDURES

This is where you develop all the relevant policy documents and other supporting documents that will ultimately form part of your ISMS. It is worth thinking about how you will organise and control the ISMS documents.

Depending on the size and complexity of your organization, this has potential to impact the quantity of ISMS documents required, and as such may affect your decision on how you will control and manage the ISMS documents, maybe through using a simple network folder structure, or using tools like SharePoint or dedicated ISMS management tools.

STEP SEVEN

OPERATIONAL

PLANNING PROCESSES

At this stage you will need to identify the Annex A controls (inset) that you have decided to apply to specific risks, and those that require new ISMS policies, processes, or procedures.

IMPLEMENTING ACTIONS

The standard requires you to think about the way in which external and internal issues can affect its ability to achieve the intended outcome(s) of its information security management system. The majority of these may be included in the risk assessment process but there may be other factors that may also need to be considered.

The needs and expectations of interested parties also have a bearing on the ISMS, as well as risks and their treatment.

RISK ASSESSMENT REVIEW

The organization needs to set as part of its risk policy and procedure the frequency with which it will review the risk assessments and treatment plan and monitor the status of mitigating actions and controls.

STEP EIGHT

PERFORMANCE REVIEW

INTERNAL AUDITS

Maintaining process conformity and continual improvement are essential – you have spent time, effort and financial resources working towards or achieving an ISO certification, and one of the most difficult things is maintaining it. Internal audits are a way of ensuring that the defined processes continue to be implemented as intended and that they reflect process changes that may result from adopting new technologies, and variations in business operations or key staff.

It is important to develop in the implementation stages an audit programme that covers off all areas of the standard and the policies, processes, and procedures that are in scope. All these areas need evidence of auditing before you proceed to having your certification audit with your chosen RCB.

Internal audits can be achieved by suitably trained auditors within your organization or by outsourced internal audit services provided by a 3rd party.

One other useful thing to undertake is an internal pre-certification audit which is a good way of assessing your readiness for going ahead with a formal certification, and to determine if you still have any compliance gaps.

Internal audits should involve a thorough review of your organization's operations

REVIEW OBJECTIVES

At this stage of your implementation programme, it is important to reaffirm and adjust any of the ISO27001 objectives if required.

Progress against objectives should be updated and tracked.

MANAGEMENT REVIEW

If you haven't already held a management review meeting, then it is important to perform at least one or ideally more if possible before your certification assessment.

Things to ensure:

- The management review covers off as a minimum the requirements as stated in clause 9.3 of the standard, in particular sub-points 9.3a, b, c, d, e and f.
- Key stakeholders attend and contribute to the review and that top management is involved in the meeting agenda
- That you maintain minutes and key actions from the review

Management reviews are an important part of being certified to ISO27001

CORRECTIVE ACTION

Nonconformities and associated corrective actions come from several sources such as:

- Internal audits
- Security incidents
- External customers or interested parties
- Internal staff from improvement suggestions
- Management Review and other internal review activities

Always ensure that you have appropriate procedures and mechanisms in place for recording and tracking nonconformities and the corrective actions taken, as these are key records required from the management system requirements.

STEP NINE

GAP ASSESSMENT PLANS AND ACTIONS

UPDATE GAP ANALYSIS

Ensure that the gap analysis that was done previously shows 100% or as high a completion as is possible at this point for the areas of assessment against the standard.

ASSIGN RESPONSIBILITIES

All gap assessment actions should be assigned to individuals who are competent and appropriate to address them to closure.

ADDRESS OPEN ACTIONS

Confirm that actions from gap assessments have all been addressed and closed out. Verify that any actions that resulted in new ISMS policies/procedures have been completed and that these are fully incorporated into the ISMS repository.

UPDATE PLAN PROGRESS

Whoever is managing and driving the ISO27001 implementation should verify task completion against the implementation plan and the status of the above gap analysis actions.

Any issues or roadblocks to progress should be raised with the steering group and where appropriate the executive sponsor.

MANDATORY PROCEDURES

There are several procedures which are required by the ISO27001 standard and associated controls, such as the Statement of Applicability and asset inventory. All of these should be issued and as few as possible should be in a draft state before a Stage 1 audit.

RISKS AND ACTIONS

Check that the risk treatment plan is up-to-date and that actions are being monitored and progressed.

ISSUE AND APPROVAL

Check that the ISMS contains fully issued and approved documents as much as is reasonably possible at this point. It is acceptable that there are working draft documents at any point in time, but it looks bad if you proceed to a certification audit with most of the ISMS in draft or with unpublished policies and documents.

ASSET LISTS UPDATED

Check that the assets list has been fully populated, and any newer assets acquired, or other information assets that have come to light, are added as necessary.

STEP TEN

PLANNING YOUR CERTIFICATION NEEDS

SELECT A CERTIFICATION BODY

At this point you may like to get in touch with a Registered Certification Body (RCB) who will be able to carry out the certification audit later. We would recommend you choose an accredited RCB reasonably early and start to get to know them, including when they are available and how much they charge. This prevents surprises later.

COSTS AND BUDGET

The initial certification costs will be driven by several factors such as the number of sites and employees, and the industry you are in. The cost of maintaining your certification also needs to be factored in.

At this point you should be ready to select your preferred RCB and start to prepare your assessment dates.

AUDITS AND ASSESSMENTS

A key aspect of ISO27001 is the need to perform internal audits of the ISMS. Before any RCB certification assessment you should have completed, or at least be well under way to completing, audits of all aspects of your ISMS against the ISO27001 standard.

PREPARING FOR AUDIT

Once preparations are done, you’re ready for the auditor to make an appearance from the certification body. This happens in two stages, conveniently called Stage One and Stage Two. Stage One is a document review to see how ready you are and how well your scope is defined. If the Stage One review encounters no major issues, then you will be able to set a date for the Stage Two certification visit. If this is completed successfully, then certification has been achieved and all your hard work has come to fruition.