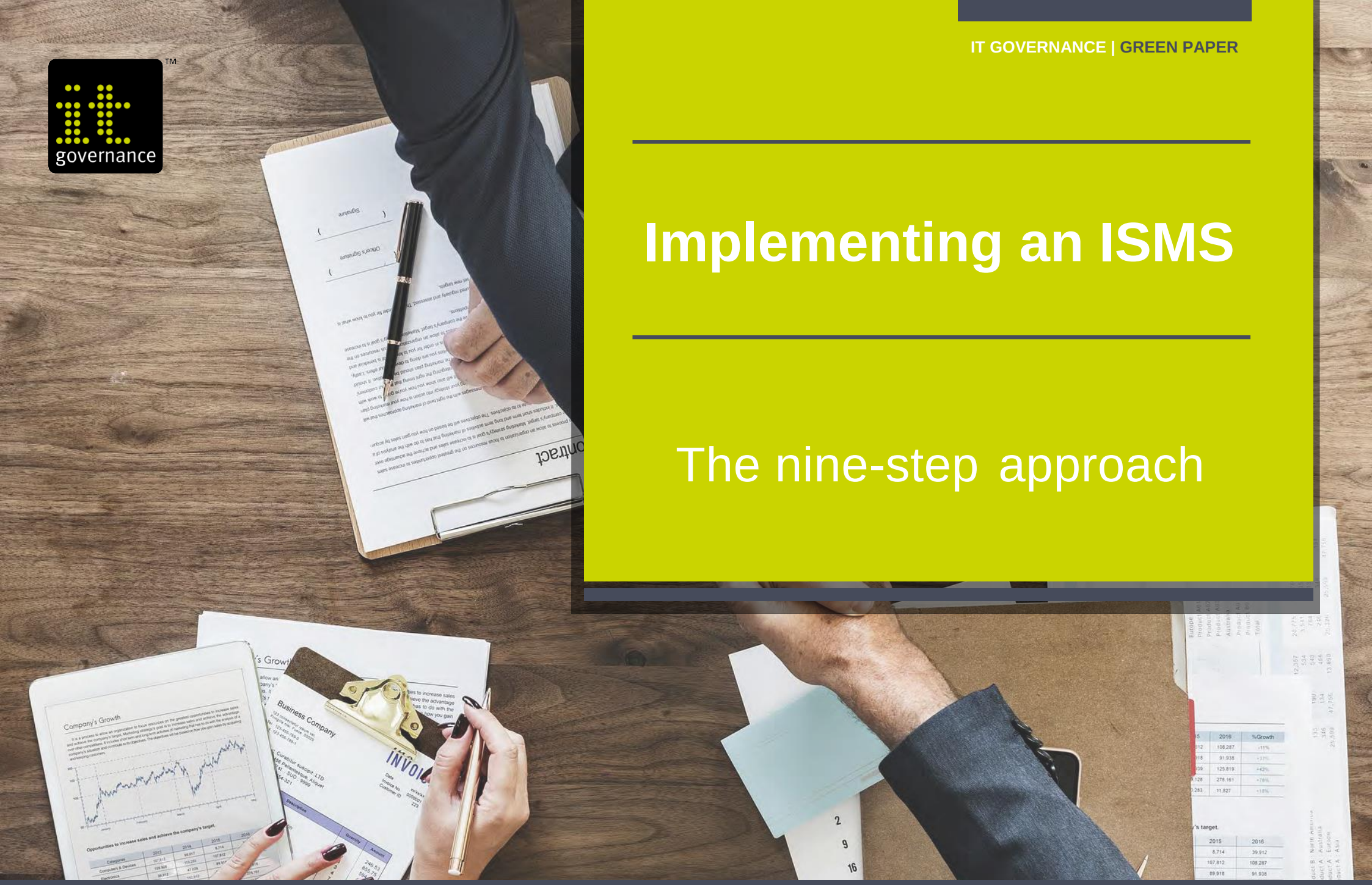


IT GOVERNANCE | GREEN PAPER

# Implementing an ISMS

## The nine-step approach

Protect • Comply • Thrive

# Introduction

Information security is not just about antivirus software, implementing the latest firewall, or locking down your laptops and web servers – it is just as much about addressing risks without compromising your business objectives. Because of this, the overall approach to information security should be strategic as well as operational.

An information security management system (ISMS) is a systematic approach to managing confidential or sensitive company information so that it remains secure.

The fact that it is systematic is possibly the most important facet of an ISMS: it protects the organization's information by ensuring consistent, effective behaviors. If an organization knows how it needs to operate in order to keep information secure, creating a system to ensure this happens is a key to success.

For an organization to secure its information, it must approach the task from the perspectives of people, processes, and technologies. These are interlinked. In the simplest sense, a technology needs a person to manage and maintain it, and that person needs to follow defined processes in doing so.

This is part of the systematization of information security: ensuring full coverage at any point that information could be compromised.

# Implementation is a project

While many organizations develop a range of security measures as they grow, and many of those measures are effective, these information security regimes are often disjointed, and gaps will inevitably be discovered – either by the organization or by its enemies.

Developing a comprehensive, effective ISMS to secure your organization's information assets is almost inevitably a large undertaking. It will require the organization to treat it as a major project, with all of the associated trappings, such as securing management commitment, defining project governance, setting outcomes and timescales, and ensuring adequate resources are available and earmarked.

# Nine steps

The IT Governance nine-step approach to implementing an ISO 27001-compliant ISMS takes all of this into account, and reflects the methodology used by our consultants in hundreds of successful ISMS implementations around the world.

This paper cannot possibly cover all the possible issues you might encounter, or spell out every incremental step, but it does describe what we consider the essential implementation process.

The nine steps cover the full extent of the project, from initial discussions with managers through to testing the completed project. It is as much about having the board on your side as it is about implementing security controls.

It is important to remember that this process is not exhaustive. Each organization will come up against its own set of stumbling blocks and will need to consult other sources of information.

While this approach is focused on achieving accredited certification, this is not strictly necessary for an organization to get significant value from its ISMS. To realize maximum value, however – such as from improved business opportunities, simpler compliance with legal and regulatory requirements, and so on – certification should certainly be a consideration.

The nine-step process is described in more detail in Nine Steps to Success – An ISO27001:2013 Implementation Overview.

## Step 1. Project mandate

The first, obvious step is to start. Starting any project is a critical phase succinctly explained with a cliché: well begun is half done.

The project leader will, at least initially, be the person who takes the initiative and begins the push for the ISMS. They will be the person to whom everyone else in the organization looks for information and guidance on the project.

The project mandate itself is essentially a set of answers to the questions all projects face in their early stages:

- What are we hoping to achieve?
- How long will it take?
- What will it cost?
- Does it have management support?

The last of these is proof that the first three have been clearly answered, and it is absolutely essential. Success depends entirely on the project having real support from the top of the organization.

Developing the answers to these questions may involve a lot of research and preparation – gap analyses, budgeting, reviewing case studies, and so on. This is time well spent, though, because a failure to adequately prepare will likely mean that you will be unable to meet your objectives.

A deliverable for this step will be a set of documents laying out the project. A project initiation document (PID) would be an ideal format for the mandate to take.

## Step 2. Project initiation

With the mandate in place, the next step is to set up the project and the project governance structure, as described in Nine Steps to Success. This is essentially an extension of what is contained in the PID, comprising:

- Information security objectives
- The project team
- A project plan
- A project risk register

The information security objectives are more granular and specific than the project objectives set in the previous step. They will feed into the information security policy and really shape how the ISMS is applied. Because these are 'policy-level' objectives, they should include a time-bound statement about whether the organization is seeking certification or just compliance with the Standard.

The project team should represent the interests of every part of the organization and various levels of seniority. You should also draw up a RACI matrix at this point, identifying who is responsible, accountable, consulted, and informed regarding the key decisions relating to the project.

A key role is that of the information security manager. In addition to having a central role in the implementation project, they will eventually be responsible for the day-to-day functioning of the ISMS.

The project plan is part of the process of gradually drilling down into what will actually be done in implementing ISO 27001, and should include critical project data such as review dates. Additional resources and information may be necessary to make sure that the plan is comprehensive and suitably detailed.

The risk register should account for risks to the project itself. These might be budgetary (will the organization continue to fund the project?), cultural (will staff resist the change?), lack of management commitment (will senior management openly support the project?), legal (are there specific legal obligations that might be at risk?), and so on. Each risk included in the register should have an assigned owner and a mitigation plan, and should be reviewed regularly throughout the project.

## Step 3. ISMS initiation

ISO 27000 (the overview for the ISO information security management standards) recognizes that a “process approach” to continual improvement is the most effective model for managing information security. That is, each process has a set of inputs and outputs, and the outputs may become inputs for further processes. In a broad sense, this can be cyclical, as in continual improvement methodologies such as PDCA (Plan-Do-Check-Act).

ISO 27001 does not specify a particular continual improvement methodology, preferring instead to allow organizations to use whatever method they choose, or to use a model they already have in place. If your organization does not yet have a preferred methodology, Nine Steps to Success discusses the merits of each of the most popular models.

As part of the ISMS initiation, you will need to establish your documentation structure. We recommend a four-tier approach:

1. Policies at the very top, defining the organization’s position and requirements.
2. Procedures to enact the policies’ requirements.
3. Work instructions describing the detail for the employees who enact elements of the procedures.
4. Records tracking the procedures and work instructions, providing evidence that they have been followed correctly and consistently.

This structure is simple enough for anyone to grasp quickly, while also providing an effective way of ensuring policies are implemented at each level of the organization.

A great deal can be said about documentation, but there are two key points:

1. Documentation should be controlled to ensure the latest versions are approved and identifiable.
2. Documentation should be adequate and not excessive, enabling each process to be systematically communicated, understood, executed, and §effective.

## Step 4. Management framework

At this stage, the ISMS needs a broader sense of the actual framework. ISO 27001 addresses this in Clauses 4 and 5, requiring the organization to define the context for the ISMS, and the roles that the organization’s leadership plays.

The context of the organization is really about identifying the range of interests that need to be taken into account. The organization, clearly, has interests in information security, as do clients, partners, legal and regulatory authorities, and so on. You began examining these interests with the risk register in step 2.

As you might gather, this phase is especially important as it defines what the ISMS will eventually become. From this perspective, it is obviously important that you recognize all relevant interests so that the ISMS can meet your organization’s needs.

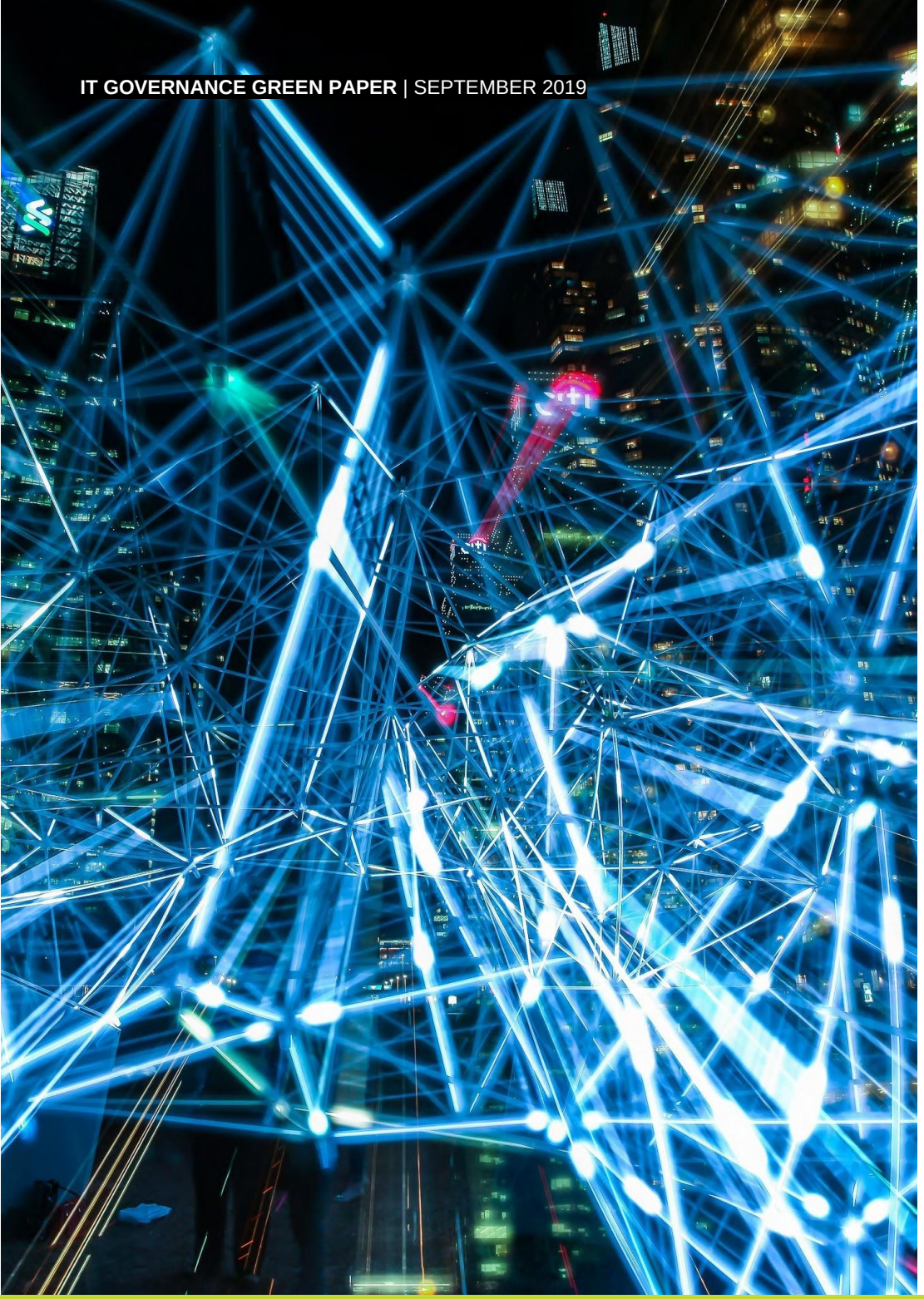
Part of this will involve identifying the scope of the ISMS, which will heavily depend on the context. The scope also needs to ensure it takes into account mobile devices and teleworkers – the organization’s logical perimeter that might be mobile, and might include devices that employees own.

The management framework also needs to set the groundwork for the rest of the implementation, so you will need to formalize some key arrangements:

- The information security policy
- The resources necessary to meet your objectives
- Your communication strategy and/or policy (both internal and external communications)
- Competence requirements

## Step 5. Baseline securitycriteria

The baseline security criteria are the core security requirements that the organization has identified. These are the requirements and corresponding measures or controls that the organization must have in place to do business. For example, a business may have a legal requirement to retain certain records; another organization may be contractually obliged to provide a minimum level of security to protect a key



customer's information assets.

This step is generally straightforward, because it operates on the basis that you have already done much of this work. You need only identify the practices you already have in place, assess their effectiveness, and ensure that they continue under the control of the eventual ISMS – potentially in an improved state.

You should, of course, ensure that you are currently meeting your obligations. Tools and databases exist that track legal requirements for information security, and you should ensure that this process covers all the necessary jurisdictions.

## Step 6. Risk management

Information security risk management is at the heart of the ISMS. On the basis of regular risk assessments, your ISMS will adapt to meet new and evolving challenges, and ensure that the risks to information security are adequately and appropriately mitigated. Risk management will need to become a core competence for any organization implementing ISO 27001.

The Standard allows the organization to broadly define its own risk management processes. Common methods focus on looking at either risks to specific assets or risks presented by specific scenarios. There are pros and cons to each, which are discussed in Nine Steps to Success, and some organizations will be considerably more suited to one method than the other.

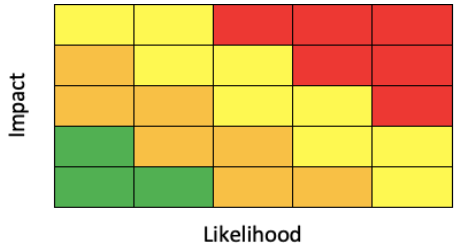
There are five important steps in an ISO 27001 information security risk assessment:

1. Establish a risk assessment framework
2. Identify risks
3. Analyze risks
4. Evaluate risks
5. Select risk management options

The risk assessment framework needs a person(s) to be responsible for the risk assessment. Without someone who is capable of performing the assessment, the whole exercise will fail.

You will also need to define your risk acceptance criteria, which involves understanding your risk appetite and the level of risk that the organization can tolerate.

Risk levels are typically calculated as a factor of the impact of a risk and its likelihood. Risk managers often present this in a simple matrix:




The results of risk analysis can be evaluated against your risk acceptance criteria to determine how you respond to the risk. Generally speaking, there are four ways of responding to a risk:

1. Tolerate the risk
2. Treat it by applying controls
3. Terminate the risk by avoiding it entirely
4. Transfer the risk, such as through insurance or agreements with other parties

For instance, your organization might decide that anything in the green area is an acceptable risk; that you will apply controls to anything orange or yellow; and anything in the red area should be terminated. You might choose to transfer some risks on a case-by-case basis.

The key outputs of an ISO 27001 risk assessment are the Statement of Applicability (SoA) and the risk treatment plan.

The SoA is a document that contains the “necessary controls” you have selected, justifications for their inclusion, whether or not they have been implemented, and justification for excluding any controls from Annex A of ISO 27001. It essentially proves that you have done due diligence by considering all the reference controls, and is especially important if you are seeking to certify your ISMS.

The risk treatment plan, meanwhile, shows the results of the risk assessment – that is, for each identified risk that requires treatment, what the organization intends to do. This should include other essential information such as responsibility for the risk and deadlines for completion.

## Step 7. Implementation

While we call this the ‘implementation’ phase, what we really refer to is the implementation of the management system processes and the risk treatment plan. This is the process of building the actual processes and security controls that will protect your organization’s information assets.

In order to ensure these are completely effective, you will need to make sure that staff are appropriately competent to operate or interact with the controls, and that they are aware of their information security obligations.

You will need to develop a process to manage the competences necessary to achieve your ISMS objectives. Competence should take into account not only the specific skills and knowledge needed for the relevant controls but also a strong understanding of ISO 27001 and how the ISMS should operate. A small number of staff may need to acquire appropriate qualifications, focusing particularly on areas such as implementing and auditing information security, risk management, business continuity, and so on.

The Standard also requires staff, contractors, and other types of employee to be aware of the information security policy, how they contribute to effective information security management, and the implications of failing to conform to the requirements of the ISMS.

Staff are almost always the organization’s weakest point, so ensuring they know how they contribute to information security is critical. Like other processes, your staff awareness program should be systematic and maintained over time.

And, of course, all of this will need to be documented. This will fall into the documentation framework you developed in the initiation phase.

This is a large and highly detailed phase of the whole implementation project; it would be wise to read up on the process and what will be required in detail.

## Step 8. Measure, monitor, and review

For the ISMS to be effective, it must meet its information security objectives. To know whether it is doing so, you need to measure, monitor, and review its performance.

ISO 27001 requires the organization to establish a series of processes that feed into the continual improvement cycle (established in step 3 – ISMS initiation):

- Monitoring, measurement, analysis, and evaluation
- Internal audit
- Management review

You will need to identify metrics or other methods of gauging the effectiveness and implementation of your processes and controls. Remember that you should not just be looking at the results, but also at elements like how often a control is used. The results should then be analyzed and evaluated to determine how effective the control actually is.

Internal audits should be scheduled at planned intervals and should cover the whole of the ISMS. It should go without saying that internal auditors need to be competent (which may require specialized training for staff, or outsourcing of the task), and that they need to demonstrate impartiality and objectivity when auditing.

Results from ongoing measurement and evaluation, and from internal audits form part of the input for the management review, alongside information about any nonconformities and corrective actions. The outputs of the review, as mentioned earlier, will be fed into the continual improvement process, allowing the organization to make corrections and adjustments to the ISMS.

## Step 9. Certification

The final step is, obviously, to have your ISMS examined and certified by an independent external body. There are several certification bodies, and the one you select should meet a couple of conditions:

- They should be accredited by your national accreditation body, which should be a member of the International Accreditation Forum (IAF).
- They should have an approach to assessment that takes each organization's circumstances into account. An ISMS is unique to its organization, and the certification audit, therefore, should not simply be a mechanical comparison of the ISMS against the Standard.

If you already have a certified management system, such as a quality or business continuity management systems (QMS, BCMS) based on an ISO standard, you should consider the value of an integrated certification service to minimize disruption and costs.

The certification audit will determine whether the ISMS is worthy of certification. There are several things you can do to maximize the likelihood of passing certification at the first attempt.

Ensure your documentation is complete, comprehensive, and available for the auditors to inspect. This should be in place before the actual certification audit, as the auditors may want to review your documentation before the visit.

Ensure that you have records of internal audits, process and control operation, and testing. These provide evidence that your ISMS is an active management system rather than just a set of documents, and may also demonstrate your corrective actions and continual improvement in action.

Make sure your staff are open and honest with the auditors, and that they know how to answer the auditors' questions. This should include ensuring appropriate staff have a thorough knowledge of the areas of information security they are responsible for.

Management should be fully involved in the certification audit. It may be useful to rehearse with them the sorts of questions they may be asked, and to review the formal, management-level policies and declarations.

For many organizations, this will be one of the most critical stages: proving that the implementation program was effective and being able to show that to partners, customers, and other stakeholders. To maximize your chances of getting to this stage, read Nine Steps to Success.


## Other papers you may be interested in


Cybersecurity – An issue for the board


Risk assessment and ISO 27001

# Useful ISMS resources

IT Governance offers a unique range of information security products and services, including books, standards, pocket guides, training courses, and professional consultancy services.

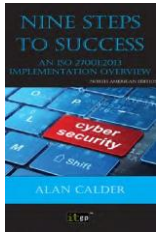
## Standards

ISO 27001 ISMS Requirements


ISO/IEC 27001:2013, usually referred to just as ISO 27001, is the best-practice specification that helps businesses and organizations throughout the world to develop an ISMS.

## Books

Nine Steps to Success – An ISO 27001:2013 Implementation Overview, North American edition




Now in its third edition, this must-have guide has been completely updated to align with IT Governance's implementation methodology, used by our consultants in hundreds of successful ISMS implementations around the world.

## Toolkits

ISO 27001 Cybersecurity Toolkit


Fulfill your ISO 27001 documentation obligations with customizable templates and implementation guidance from ISO 27001 auditors. Ensure total coverage of your project with this complete set of mandatory and supporting documentation.

## Training

Certified ISO 27001 ISMS Lead Implementer Online Training Course


If you are involved in information security management, writing information security policies, or implementing ISO 27001 – either as a Lead Implementer or as part of the planning/implementation team – this course covers all the key steps in preparing for and achieving ISMS certification first time. Also available as a distance learning course.

## Software

vsRisk Cloud – the definitive ISO 27001 risk assessment tool


Fully aligned with ISO 27001, vsRisk Cloud streamlines the risk assessment process and helps you produce robust risk assessments. The software tool saves 80% of your time and significantly cuts the consultancy costs that are typically associated with tackling a risk assessment.

# IT Governance solutions

IT Governance writes and publishes extensively on IT governance, risk management, and compliance (GRC) subjects, and has developed a range of tools for IT governance, information security, and regulatory compliance practitioners.

IT Governance is your one-stop shop for corporate and IT governance information, books, tools, training, and consultancy. Our products and services are designed to work harmoniously so you can benefit from them individually or use different elements to build something bigger and better.

## Books

We sell sought-after publications covering all areas of corporate and IT governance. Our publishing team also manages a growing collection of titles that provide practical advice for staff taking part in IT governance projects, suitable for all levels of staff knowledge, responsibility, and experience.

Visit to view our full catalog.

## Toolkits

Our unique documentation toolkits are designed to help organizations adapt quickly and adopt management best practice using customizable template policies, procedures, forms, and records.

Visit www.itgovernanceusa.com/documentation-toolkits to view and trial our toolkits.

## Training

We offer a variety of training courses, from staff awareness and Foundation courses through to advanced programs for IT practitioners and certified lead implementers and auditors.

Our training team organizes and runs in-house and public training courses all year round, as well as Live Online and distance-learning classes, covering a growing number of IT governance topics.

Visit www.itgovernanceusa.com/training for more information.

## Consultancy

We are an acknowledged world leader in our field. Our experienced consultants, with multi-sector and multi-standard knowledge and experience, can help you accelerate your IT GRC projects.

Visit www.itgovernanceusa.com/consulting for more information.

## Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organizations worldwide to be ISO 27001-compliant.

Visit www.itgovernanceusa.com/software for more information.