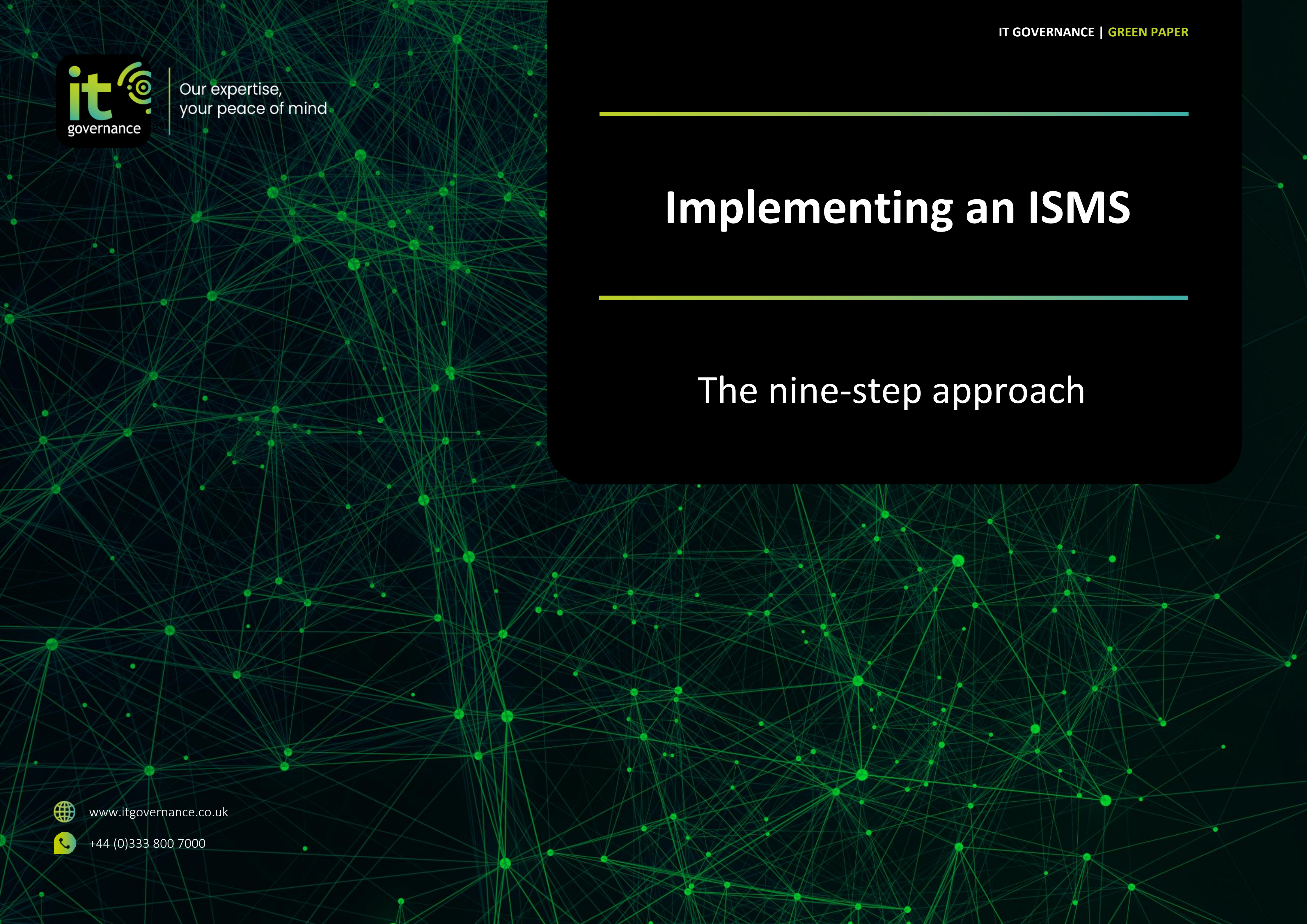


IT GOVERNANCE | GREEN PAPER

Our expertise,
your peace of mind

# Implementing an ISMS

## The nine-step approach

www.itgovernance.co.uk

+44 (0)333 800 7000

## Introduction

Information security is not simply about using the latest technology, or allocating resources so that your IT team can ‘sort it out’. True security relies on three ‘pillars’: people, processes and technology; after all, it does not do you much good to implement expensive technology only to have malware enter your systems through human error (falling for a phishing attack, for example), or for staff to not know how to use that technology effectively due to a lack of clear, documented processes.

However, even if you account for all three pillars, that in itself is no guarantee of effective – or indeed cost-effective – security. Good information security is really about addressing the risks specific to your organisation without compromising your business objectives. Your overall approach to information security should therefore be strategic as well as operational.

An information security management system (ISMS) – preferably aligned to the international standard for information security management, ISO/IEC 27001:2022 – takes a systematic approach to managing confidential or sensitive information so that it remains secure. The fact that it is systematic is perhaps the most important aspect of an ISMS: it protects the organisation’s information by ensuring consistent, effective behaviours. If an organisation knows how it needs to operate to keep its information secure, creating a system to ensure this happens is the key to success.

## Implementation is a project

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

Developing a comprehensive, effective ISMS to secure your organisation’s information assets is a large undertaking. You must treat it as a major project, with all the associated actions, such as securing management commitment, defining project governance, setting outcomes and timescales, and ensuring adequate resources are available and earmarked.

# Nine steps

Our nine-step approach to implementing an ISO 27001-compliant ISMS takes all this into account, and reflects the methodology we have used to help more than 800 organisations around the world achieve compliance with the Standard. These steps cover a complete ISO 27001 implementation project, from initial discussions to testing the finished management system and getting it certified.

While this approach is focused on achieving accredited certification, this is not strictly necessary for an organisation to get value from its ISMS. To realise maximum value, however – such as new and improved business opportunities, and simpler compliance with security-related legal and contractual requirements – organisations should consider ISO 27001 certification.

This green paper covers, in broad terms, the nine steps we consider essential to implementing an ISO 27001-compliant ISMS. These steps are discussed in more detail in Nine Steps to Success – An ISO 27001 Implementation Overview. Remember, however, that every organisation will encounter unique stumbling blocks that our broad approach cannot account for, and will need to consult other sources of information to address them.

## 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.

First, you should appoint a project leader who 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 organisation looks for information and guidance on the project.

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

- What are we hoping to achieve?
- How long will the project take?
- What resources will the project require, both financially and otherwise?
- Does the project have top management support?

Developing the answers to these questions may involve a lot of research and preparation – gap analyses, budgeting, reviewing case studies, and so on – but is time well spent. Also note the importance of the last question: securing management support is proof that the first three questions have been clearly answered. Furthermore, success depends entirely on the project having real support from the top of the organisation.

## Step 2: Project initiation

With the mandate in place, the next step is to set up the project and the project governance structure that account for your:

- Information security objectives;
- Project team;
- Project plan; and
- Project risk register.

Your information security objectives should be more granular and specific than the project objectives set in step 1. They will inform and be included in your top-level information security policy, and shape how the ISMS is applied. Your objectives should also make clear whether your organisation is seeking ISO 27001 certification or just compliance with the Standard.

The project team should represent the interests of every part of the organisation and include various levels of seniority. Drawing up a RACI matrix that identifies who is responsible, accountable, consulted and informed regarding the project's key decisions can help with this. One critical person to appoint and include in the project team is the information security manager, who will have a central role in the implementation project and eventually be responsible for the day-to-day functioning of the ISMS.

The project plan should detail the actions to take to implement the ISMS, and include information such as responsibilities, resources required, review dates and deadlines.

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

## Step 3: ISMS initiation

An important part of the ISMS initiation is establishing your documentation structure. We recommend a four-tier approach:

1. Policies at the top, defining the organisation's position and requirements.
2. Procedures to enact the policies' requirements at a high level.
3. Work instructions that set out how employees implement individual elements of the procedures. For example, a procedure may refer to a specific piece of equipment or software to use, which a work instruction can explain in more detail how to operate.
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, provides an effective way of ensuring policies are implemented at each level of the organisation and ensures that you develop well-functioning, cohesive processes. It is also important you support this simple structure with clear documentation that is systematically communicated to all areas of the business and to other stakeholders.

Your policies and procedures must also be effective, which you can achieve by:

- Keeping them practicable by balancing aspirations against the reality – if they appear too idealised, staff will be much less likely to follow them;
- Ensuring, particularly for procedures, they are clear and straightforward, so staff can easily follow them;
- Avoiding duplication; and
- Deploying version control to ensure everyone knows which is the latest document.

Besides establishing your documentation structure, you should also select a continual improvement methodology. Continual improvement is a critical element of an ISO 27001 ISMS, although the Standard does not specify any particular continual improvement methodology. Instead, it allows organisations to use whatever method they choose, so long as it "continually improve[s] the suitability, adequacy and effectiveness of the [ISMS]" (Clause 10.1). This could be a continual improvement model the organisation already uses for another activity.

## Step 4: Management framework

At this stage, the high-level framework of the ISMS needs to be developed to set the groundwork for the rest of the implementation, so you will need to formalise:

- The context for the ISMS, including:
  - Internal and external issues relevant to the ISMS (you may have already identified some in step 2);
  - Interested parties, and their needs and expectations; and
  - The ISMS scope, taking into account the two preceding points.
- How top management will demonstrate leadership and commitment to the ISMS;
- Your top-level information security policy, established by top management;
- Roles, responsibilities and authorities relevant to the ISMS;
- Your communication strategy, both internally and externally, for ISMS matters;
- Your competence requirements with respect to the ISMS; and
- The resources necessary to meet your security objectives.

## Step 5: Baseline security criteria

Next, you should formalise your baseline security criteria: the minimum level of security controls required to conduct business securely in an ISO 27001-compliant ISMS, which should account for your business, legal and contractual requirements. Tools like Compliance Manager can help ensure you identify all relevant legal requirements.

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

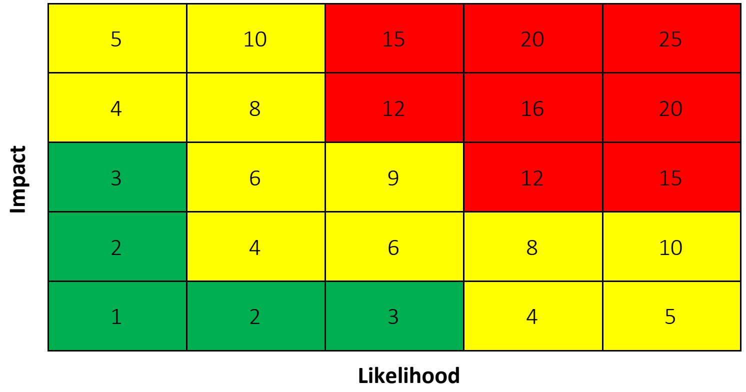
## Step 6: Risk management

Information security risk management lies at the heart of an effective ISMS, or indeed any other effective security programme. Risk assessment and management are critical for identifying what measures you need and to what degree, keeping your defences effective and affordable.

ISO 27001 requires organisations to conduct risk assessments at regular intervals and when planning significant changes, using a methodology that ensures "repeated information security risk assessments produce consistent, valid and comparable results" (Clause 6.1.2.b). Like with continual improvement, however, the exact methodology is up to the organisation, provided that it meets the Standard's requirements and accounts for the following five steps:

1. Establish and maintain information security risk criteria, including risk acceptance criteria and the criteria for performing risk assessments.
2. Identify information security risks and their risk owners.
3. Analyse the risks, assessing their potential impact and realistic likelihood to determine the risk level for each.
4. Evaluate the risks, by comparing the risk analysis results against your risk criteria and prioritising them accordingly.
5. Select risk treatment options for identified risks outside your risk appetite.

Risk levels are often presented in a matrix such as Figure 1 below, which should reflect your organisation's risk appetite. Figure 1 does this through colour-coding, where anything in the green area is an acceptable risk; anything in the yellow area requires monitoring; and anything in the red area should be mitigated as a priority.



| | | | | |
|---|---|---|---|---|
| 5 | 10 | 15 | 20 | 25 |
| 4 | 8 | 12 | 16 | 20 |
| 3 | 6 | 9 | 12 | 15 |
| 2 | 4 | 6 | 8 | 10 |
| 1 | 2 | 3 | 4 | 5 |

Impact
Likelihood

*Figure 1: Simple risk matrix example*

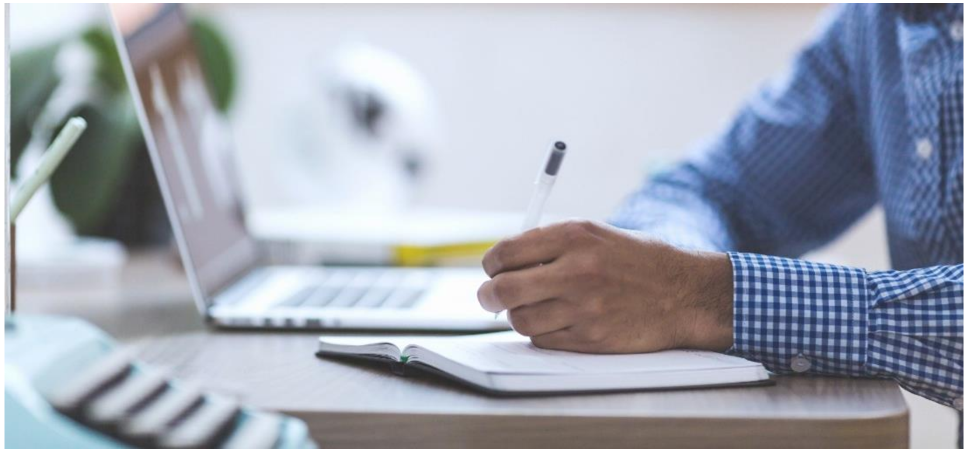
Generally speaking, there are four ways of responding to a risk:

1. Treat the risk by applying controls to bring it down to an acceptable level.
2. Transfer the risk, such as through insurance or by outsourcing the process to an organisation that is better able to manage the risk.
3. Terminate the risk by avoiding it entirely by, for example, changing the way the activity linked to the risk is conducted or even ending it altogether.
4. Tolerate the risk. This must be an active choice and have clear justification.

Make sure that you document your chosen responses, including justifications and, where applicable, control details. It is also an ISO 27001 requirement to compare the controls against those in Annex A (a list of information security controls at the end of the Standard, which are described in more detail, along with implementation guidance, in ISO 27002) to verify that no necessary controls have been omitted.

A key output of this process is the Statement of Applicability (SoA): 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 Annex A controls. It essentially proves that you have done due diligence by considering all the Standard's reference controls, and is especially important if you are seeking to certify your ISMS.

Another key output is a risk treatment plan, which should show the results of the risk assessment process, as well as other essential information such as the risk owners and risk treatment deadlines. It is also an explicit ISO 27001 requirement to obtain risk owners' approval of the plan, as well as their acceptance of the residual risks. Remember: your risk treatments only need to bring the risks down to an acceptable level, and not necessarily eliminate the risks.



## Step 7: Implementation

The ‘implementation’ phase relates to implementing the management system processes and risk treatment plan – in other words, building the actual processes and security controls that will protect your organisation’s information assets. Those processes and controls should also be documented in relevant policies, procedures, work instructions and records, as outlined in step 3.

To ensure those processes and controls will be effective, you need to make sure that staff are appropriately competent to implement, operate or interact with, and maintain the controls. You have already established your competence requirements in step 4; now you need to, where you do not yet have them, take actions to acquire those competences, such as providing the necessary training. You will also need to develop and implement a process for managing those competences.

ISO 27001 also requires staff and other persons doing work under your organisation’s control to be aware of your information security policy, how they contribute to the effectiveness of the ISMS, and the implications of failing to conform to the ISMS requirements. Staff are almost always an organisation’s weakest point when it comes to security, so ensuring they understand their security obligations and how they can help keep the organisation safe is critical. Like your other processes, your staff awareness programme should be systematic and maintained over time.

## 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 monitor, measure, analyse and evaluate its performance. This requires you to identify metrics or other methods – that “produce comparable and reproducible results” (Clause 9.1.b) – of gauging the effectiveness and implementation of your processes and controls. You must also document, analyse and evaluate the results to determine the effectiveness.

ISO 27001 also requires organisations to conduct regular internal audits, covering the whole ISMS, as part of an audit programme to confirm that the ISMS:

- Has been implemented effectively;
- Is being maintained effectively; and
- Is meeting its objectives as well as the requirements outlined in the Standard.

Naturally, the auditors need to be objective and impartial. To ensure the latter, outsourcing could be a good option. Alternatively, to ensure internal staff have the right competence, specialised training may prove invaluable.

ISO 27001 also requires top management to regularly review the ISMS “to ensure its continuing suitability, adequacy and effectiveness” (Clause 9.3.1). This review must take into account:

- The status of actions from previous management reviews;
- Changes in internal and external issues, or in the needs and expectations of interested parties;
- Feedback from your measurement activities, internal audits and interested parties;
- Information about any nonconformities, corrective actions and opportunities for improvement; and
- Risk assessment results, and the status of the risk treatment plan.

The outputs of measurement, internal audits and management reviews must be fed into the continual improvement process, allowing the organisation to make corrections and adjustments to its ISMS.

## Step 9: Certification

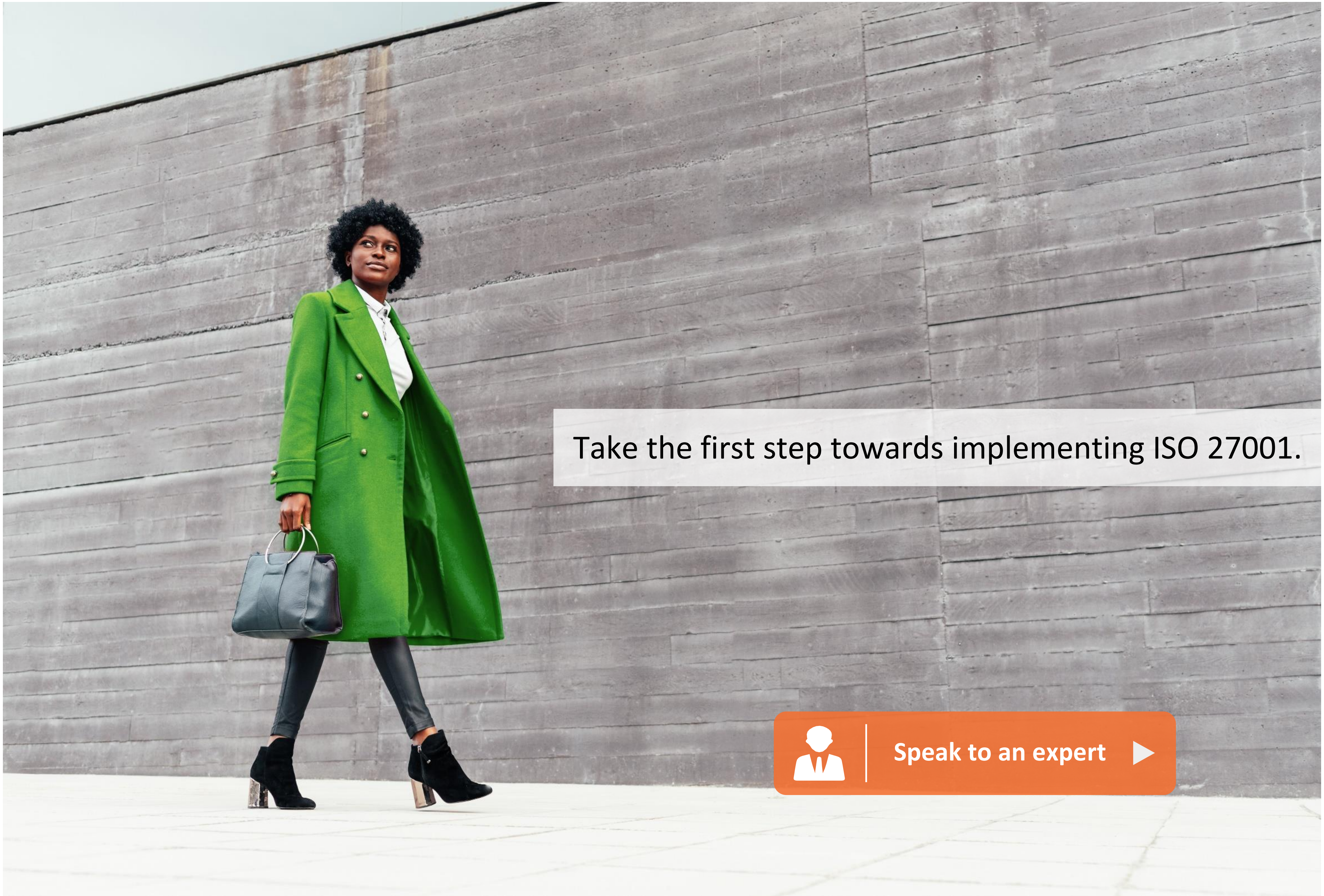
The final step is to have your ISMS examined and certified by an independent external body. There are many certification bodies to choose from, though you should make sure it is accredited by your national accreditation body, which should be a member of the International Accreditation Forum (IAF). Any certificate awarded by an unaccredited certification body is unlikely to be recognised by other parties.

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

The certification audit will determine whether the ISMS is worthy of certification. There are several things you can do to maximise 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, processes, control operations 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.
- Interviews are a significant part of the audit, so make sure staff with ISMS responsibilities are available to speak with the auditors, are open and honest with them, and know how to answer the auditors' questions. Where staff lack the auditee experience, practice or mock interviews can help build their confidence.
- Management should also be involved in the certification audit, as their commitment to the ISMS is an ISO 27001 requirement and vital for an effective management system.

For many organisations, certification will be one of the most critical stages: proving that the implementation programme was effective and being able to show that to partners, customers and other stakeholders. Certification is also what will realise the maximum value from implementing ISO 27001 discussed earlier: providing new and improved business opportunities, and offering simpler compliance with security-related legal and contractual requirements.



Take the first step towards implementing ISO 27001.

Speak to an expert ▶

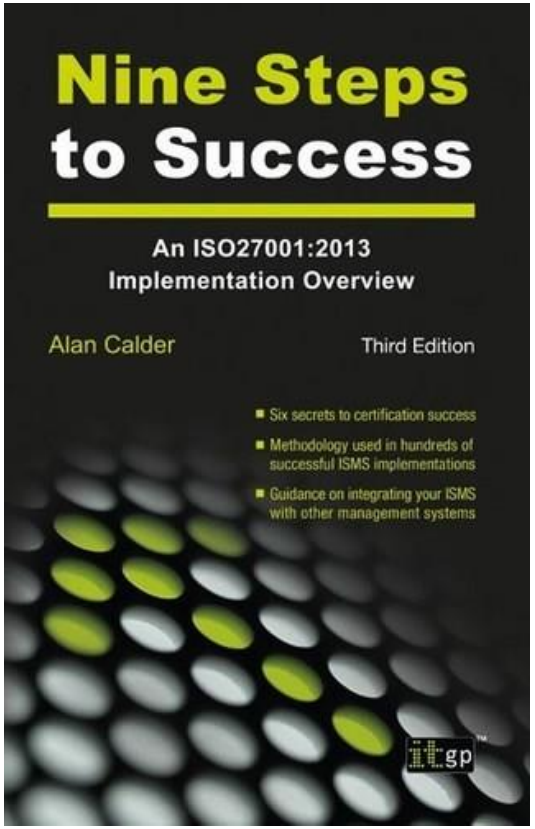
# Nine Steps to Success

## An ISO 27001 Implementation Overview

Now in its third edition, this must-have guide by ISO 27001 expert Alan Calder helps you get to grips with the requirements of the Standard and make your ISO 27001 implementation project a success.

## This book will help you:

- Secure management support;
- Create a management framework;
- Perform a gap analysis to understand the controls you have in place and identify where to focus your implementation efforts and resources;
- Structure and resource your project, including by:
  - Examining the tools and resources available; and
  - Advising on whether and when to use consultants.
- Conduct a five-step risk assessment;
- Create an SoA and a risk treatment plan;
- Integrate your ISMS with other management systems aligned to an ISO standard;
- Address challenges with creating documentation; and
- Continually improve your ISMS, including via:
  - Internal audits;
  - Testing; and
  - Management review.


Nine Steps to Success
An ISO27001:2013 Implementation Overview
Alan Calder
Third Edition
Six secrets to certification success
Methodology used in hundreds of successful ISMS implementations
Guidance on integrating your ISMS with other management systems
itgp

Find out more ▶

# Useful ISO 27001 resources

IT Governance offers a unique range of ISO 27001 products and services, including standards, documentation toolkits, software tools, consultancy services and training courses.

INTERNATIONAL STANDARD
ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection - Information security management systems - Requirements
ISO
IEC

## ISO/IEC 27001:2022 Standard

Download the 2022 edition of ISO/IEC 27001 (*Information security, cybersecurity and privacy protection — Information security management systems — Requirements*), the international standard for information security management that provides the specification for a best-practice ISMS, covering organisational, people, physical and technological controls.

## ISO 27001 Toolkit

Save hours of work in your ISMS implementation project with more than 140 customisable, ISO 27001-compliant documentation templates and expert guidance. You can further accelerate your project with the included gap analysis tools, which will help you understand what needs to be done to achieve ISO 27001 certification.

This toolkit is hosted on our Cloud-based DocumentKits platform, allowing for easy collaboration.

## vsRisk

Simplify and speed up the ISO 27001 risk assessment process with vsRisk, a Cloud-based information security risk assessment tool developed by industry-leading experts. Saving you up to 80% of your time conducting risk assessments, this software tool accelerates compliance with ISO 27001, helping you produce accurate, auditable and hassle-free risk assessments year after year. The built-in libraries of risks and controls ensure completeness, and the simple, intuitive dashboard helps you track and mange key risks.

## ISO 27001 Gap Analysis

Have a specialist review your current security measures against the ISO 27001 requirements to get the true picture of your compliance posture, and receive a detailed gap analysis report with our consultant's findings and recommendations for remediating any compliance gaps. The report also provides options for your ISMS scope, and how they can help meet your business and strategic objectives, as well as an outline action plan and indications of the level of internal management effort required to implement an ISMS.

## Certified ISO 27001:2022 ISMS Foundation Training Course

Learn from the people who led the world's first successful ISO 27001 implementation project. This one-day course provides a comprehensive introduction to the features and benefits of ISO 27001:2022, and teaches you how to plan, scope and communicate throughout your ISO 27001 project, the key steps involved in risk assessment, the necessary documentation, and more. Learn in person, or choose from Live Online or self-paced online formats.

## Certified ISO 27001:2022 ISMS Lead Implementer Training Course

Train with the ISO 27001 experts on this three-day course, and gain the skills to lead and manage an ISO 27001-compliant ISMS implementation project. The course teaches the nine critical steps involved in planning, implementing and maintaining an effective ISMS, information security management best practices, how to structure and manage your ISO 27001 project, and how to deal with typical pitfalls and challenges. Learn in person, or choose from Live Online or self-paced online formats.

# More free green papers

IT Governance publishes numerous free green papers – as well as many other resources, including webinars, infographics and case studies – on a wide range of topics. Here are two you might be interested in:

IT GOVERNANCE | GREEN PAPER

Risk Assessment and ISO 27001

September 2019

Protect • Comply • Thrive

## Risk Assessment and ISO 27001

Want to learn more about how to conduct a risk assessment in line with ISO 27001? This green paper walks you through five simple steps to produce reliable and robust risk assessment results, and explains how to resolve typical challenges you may face during the risk assessment process.

IT GOVERNANCE | GREEN PAPER

ISMS Measurement

Metrics made easy

Protect • Comply • Thrive

## ISMS Measurement – Metrics made easy

Want to learn more about how to measure your ISMS effectively? This green paper discusses the key principles of effective measurement, including how to prioritise controls. It also describes some of the common pitfalls encountered when developing and operating a measurement system under ISO 27001, and how to avoid them.

**About IT Governance green papers**

The concept of "Our expertise, your peace of mind" informs everything we do – sharing our knowledge and experience to ensure our customers' IT governance, risk management and compliance (GRC) projects go smoothly and are successful.

Our green papers draw on our specialists' experience and expertise to give you the guidance you need to move your projects forward, whether you need expert advice on compliance, a concise guide to a tricky process or tips for implementing management systems.

IT Governance green papers: the green light at the start of your IT GRC journey.

**Visit our resource hub ▶**

# IT Governance solutions

IT Governance is your one-stop shop for cyber security and IT GRC information, books, documentation toolkits, training, consultancy, penetration testing, software tools, and more. Our products and services work harmoniously together so you can use them individually or combine different elements depending on your needs.

## Books

Our sister company IT Governance Publishing (ITGP) is the world's only niche IT governance publisher, collaborating with industry experts to produce high-quality publications about best-practice frameworks, compliance and technical subjects.

Our books cover a wide range of GRC topics, including cyber security and resilience, data privacy and business continuity. They also come in a range of formats, including softcover, PDF, ePub, Kindle and audiobook.

Visit www.itgovernance.co.uk/shop/category/itgp-books to view our full catalogue.

## Toolkits

Created by expert practitioners and used by more than 17,000 organisations worldwide, our toolkits contain fully customisable documentation templates designed to help you meet your compliance obligations, ranging from ISO 27001 to the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Cyber Essentials, ISO 22301, and more.

Each toolkit is hosted on our Cloud-based DocumentKits platform, enabling us to regularly update them and making it easier for you to collaborate. The toolkits also come with unlimited support for account setup and assistance to help you customise and use the templates.

Visit www.itgovernance.co.uk/documentation-toolkits to view all our toolkits.

## Training

We provide a wide range of training courses, covering areas including data privacy, information security and ISO 27001, cyber security, ethical hacking, and professional certification courses such as CISA®, CISM®, CGEIT® and CRISC®. To date, we have trained more than 28,000 individuals.

Our courses range from introductory to advanced training, and are available as classroom, Live Online and self-paced online courses. Visit www.itgovernance.co.uk/training for more information.

More interested in short awareness courses that deliver a consistent, interactive and comprehensive message to all your staff? Visit www.itgovernance.co.uk/staff-awareness-e-learning-courses for more information.

## Consultancy

Whatever your IT GRC needs and budget, we have consultancy options to suit you. From fixed-price packaged solutions to bespoke and corporate consultancy services, we can help you meet your objectives efficiently and cost-effectively.

Our unique combination of technical expertise and practical experience managing hundreds of projects around the world means we can deliver a complete solution, managing your project from start to finish. Join the more than 5,000 organisations we have already helped, and let us offer you cost-saving and risk-reducing solutions based on international best practice and frameworks.

Visit www.itgovernance.co.uk/consulting for more information.

## Penetration testing

Identify and mitigate your vulnerabilities before criminal hackers can exploit them. Our CREST-accredited penetration testing solutions can support your organisation's security by identifying vulnerabilities in your infrastructure, applications, wireless networks and people through our fixed-price penetration testing packages.

At the end of each engagement, you will receive a comprehensive report that clearly explains any issues we have identified from both technical and non-technical perspectives, how those issues affect your organisation, and recommendations for remediating them.

Visit www.itgovernance.co.uk/penetration-testing-services for more information.

## Software

Our sister company Vigilant Software develops industry-leading software tools designed to make meeting your security obligations and complying with privacy laws simple and affordable.

The CyberComply platform comprises six Cloud-based tools: Compliance Manager, the Data Flow Mapping Tool, the Data Protection Impact Assessment (DPIA) Tool, GDPR Manager, Incident Manager and vsRisk.

Visit www.itgovernance.co.uk/shop/category/software for more information.

## IT Governance Ltd

Unit 3, Clive Court, Bartholomew’s Walk
Cambridgeshire Business Park, Ely
Cambs., CB7 4EA, United Kingdom

www.itgovernance.co.uk
+44 (0)333 800 7000
servicecentre@itgovernance.co.uk

/it-governance
@ITGovernance
/ITGovernanceLtd