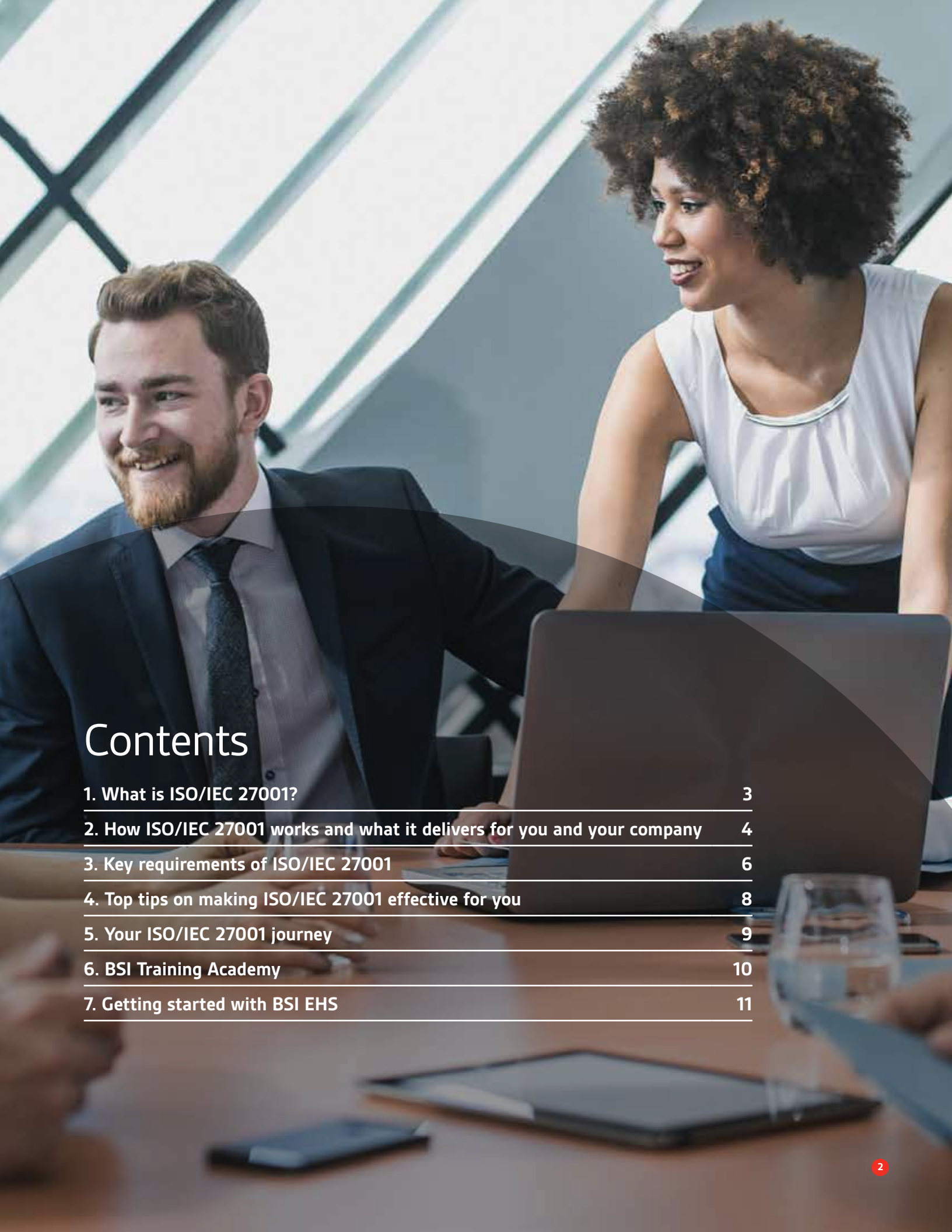
Your Implementation Guide

ISO/IEC 27001

bsi.

...making excellence a habit.™



Contents

Your implementation guide to **ISO/IEC 27001**

1. What is ISO/IEC 27001?

Successful businesses understand the value of timely, accurate information, good communications and confidentiality. Information security is as much about exploiting the opportunities of our interconnected world as it is about risk management.

That's why organizations need to build resilience around their information security management. Internationally recognized **ISO/IEC 27001** is an excellent framework, which helps organizations manage and protect their information assets so that they remain safe and secure.

At BSI, we have the experience, the experts and the support services to help make sure you get the most from **ISO/IEC 27001**, by making you more resilient and responsive to threats to your information.

This guide shows you how to implement **ISO/IEC 27001** in your organization to build resilience for the long term and safeguard your reputation. We also showcase our additional support services, which help you not only achieve compliance, but continue to reduce risk and protect your business.

"ISO/IEC 27001 demonstrates to clients that we have secure data and robust systems."

– **Hugo Holland Bosworth**
Group Operations Director, Alternative Networks Plc

Your implementation guide to **ISO/IEC 27001**

2. How **ISO/IEC 27001** works and what it delivers for you and your company.

The ability to manage information safely and securely has never been more important. ISO/IEC 27001 not only helps protect your business, it also sends a clear signal to customers, suppliers and the marketplace that your organization has the ability to handle information securely.

ISO/IEC 27001 is a robust framework that helps you protect information such as financial data, intellectual property or sensitive customer information. It helps you identify risks and puts in place security measures that are right for your business, so you can manage or reduce risks to your information. It helps you to continually review and refine the way you do this, not only for today, but also for the future. That's how ISO/IEC 27001 protects your business, your reputation and adds value.

"It helped the team understand the threats and vulnerabilities that exist in today's environment and proactively control them. It has led to a greater awareness, vigilance and enthusiasm for information security."

– **Mr. Tareq Al-Sahaf,**
General Manager. Gulf Insurance Group K.S.C (GIG)

Benefits of ISO/IEC 2001:2013*

75%
reduces business risk

80%
inspire trust in our business

71%
helps protect our business

55%
helps us comply with regulations

53%
increases our competitive edge

50%
reduces likelihood of mistakes

**Source – BSI voice of the customer 2012-2016*

Your implementation guide to **ISO/IEC 27001**

How ISO/IEC 27001 works

The latest version of ISO/IEC 27001 was published in 2013 to help maintain its relevance to the challenges of modern day business and ensure it is aligned with the principles of risk management contained in ISO 31000. It's based on the high level structure (Annex SL), which is a common framework for all revised and future ISO management system standards, including ISO 9001:2015 and ISO 14001:2015.

Annex SL helps keep consistency, align different management system standards, offer matching sub-clauses against the top level structure and apply a common language. It compels organizations to incorporate their Information Security Management System (ISMS) into core business processes, make efficiencies and get more involvement from senior management.

Some of the core concepts of ISO/IEC 27001:2013 are:

Concept	Comment
Context of the organization	Consider the combination of internal and external factors and conditions that can affect the organization's information.
Issues, risks and opportunities	Issues can be internal or external, positive or negative and include conditions that affect the confidentiality, integrity and availability of an organization's information. Risks are defined as the "effect of uncertainty on an expected result".
Interested parties	A person or entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity. Examples include suppliers, customers or competitors.
Leadership	Requirements specific to top management who are defined as a person or group of people who directs and controls an organization at the highest level.
Risk associated with threats and opportunities	Refined planning process replaces preventive action and is defined as the "effect of uncertainty on an expected result".
Communication	The standard contains explicit and detailed requirements for both internal and external communications.
Documented information	The meaningful data or information you control or maintain to support your ISMS.
Performance evaluation	The measurement of the ISMS and risk treatment plan effectiveness.
Risk owner	The person or entity that has been given the authority to manage a particular risk and is accountable for doing so.
Risk treatment plan	A risk modification plan which involves selecting and implementing one or more treatment options against a risk.
Controls	Any administrative, managerial, technical or legal method that is used to modify or manage an information security risk. They can include things like practices, processes, policies, procedures, programs, tools, techniques, technologies, devices and organizational structures. They are determined during the process of risk treatment.
Continual improvement	Methodologies other than Plan-Do-Check-Act (PDCA) may be used.

3. Key requirements of **ISO/IEC 27001**

Clause 1: Scope
The first clause details the scope of the standard.

Clause 2: Normative references
All the normative references are contained in ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary, which is referenced and provides valuable guidance.

Clause 3: Terms and definitions
Please refer to the terms and definitions contained in ISO/IEC 27000. This is an important document to read.

Clause 4: Context of the organization
This is the clause that establishes the context of the organization and the effects on the ISMS. Much of the rest of the standard relates to this clause.

The starting point is to identify all external and internal issues relevant to your organization and your information or information that is entrusted to you by 3rd parties. Then you need to establish all "interested parties" and stakeholders as well as how they are relevant to the information. You will need to identify requirements for interested parties, which could include legal, regulatory and/or contractual obligations. You'll also need to consider important topics such as any market assurance and governance goals.

You will be required to decide on the scope of your ISMS, which needs to link with the strategic direction of your organization, core objectives and the requirements of interested parties.

Finally, you'll need to show how you establish, implement, maintain and continually improve the ISMS in relation to the standard.

Clause 5: Leadership
This clause is all about the role of "top management," which is the group of people who direct and control your organization at the highest level. They will need to demonstrate leadership and commitment by leading from the top.

Top management needs to establish the ISMS and information security policy, ensuring it is compatible with the strategic direction of the organization. They also need to make sure that these are made available, communicated, maintained and understood by all parties.

Top management must ensure that the ISMS is continually improved and that direction and support are given. They can assign ISMS relevant responsibilities and authorities, but ultimately they remain accountable.

Clause 6: Planning
This clause outlines how an organization plans actions to address risks and opportunities to information.

It focuses on how an organization deals with information security risk and needs to be proportionate to the potential impact they have. ISO 31000, the international standard for risk management, contains valuable guidance. Organizations are also required to produce a "Statement of Applicability" (SoA). The SoA provides a summary of the decisions an organization has taken regarding risk treatment, the control objectives and controls you have included and those you have excluded, and why you have decided to include and exclude the controls in the SOA.

Another key area of this clause is the need to establish information security objectives and the standard defines the properties that information security objectives must have.

Clause 7: Support
This section of ISO/IEC 27001 is all about getting the right resources, the right people and the right infrastructure in place to establish, implement, maintain and continually improve the ISMS.

It deals with requirements for competence, awareness and communications to support the ISMS and it could include making training and personnel available, for example. This clause also requires all personnel working under an organization's control to be aware of the information security policy, how they contribute to its effectiveness and the implications of not conforming.

The organization also needs to ensure that internal and external communications relevant to information security

and the ISMS are appropriately communicated. This includes identifying what needs to be communicated to whom, when and how this is delivered.

It's in this clause that the term "documented information" is referenced. Organizations need to determine the level of documented information that's necessary to control the ISMS. There is also an emphasis on controlling access to documented information, which reflects the importance of information security.

Clause 8: Operation

This clause is all about the execution of the plans and processes that are the subject of previous clauses.

It deals with the execution of the actions determined and the achievement of the information security objectives. In recognition of the increased use of outsourced functions in today's business world, these processes also need to be identified and controlled. Any changes, whether planned or unintended need to be considered here and the consequences of these on the ISMS.

It also deals with the performance of information security risk assessments at planned intervals, and the need for documented information to be retained to record the results of these.

Finally, there is a section that deals with the implementation of the risk treatment plan, and again, the need for the results of these to be retained in documented information.

Clause 9: Performance evaluation

This clause is all about monitoring, measuring, analyzing and evaluating your ISMS to ensure that it is effective and remains so. This clause helps organizations to continually assess how they are performing in relation to the objectives of the standard to continually improve.

You will need to consider what information you need to evaluate the information security effectiveness, the methods employed and when it should be analyzed and reported.

Internal audits will need to be carried out as well as management reviews. Both of these must be performed at planned intervals and the findings will need to be retained as documented information.

It should be noted that management reviews are also an opportunity to identify areas for improvement

Clause 10: Improvement

This part of the standard is concerned with corrective action requirements. You will need to show how you react to nonconformities, take action, correct them and deal with the consequences. You'll also need to show whether any similar nonconformities exist or could potentially occur and show how you will eliminate the causes of them so they do not occur elsewhere.

There is also a requirement to show continual improvement of the ISMS, including demonstrating the suitability and adequacy of it and how effective it is. However you do this is up to you.

ISO/IEC 27001 also includes Annex A which outlines 114 controls to help protect information in a variety of areas across the organization. ISO/IEC 27002 also provides best practice guidance and acts as a valuable reference for choosing as well as excluding which controls are best suited for your organization.

4. Top tips on making **ISO/IEC 27001** effective for you.

Every year we help tens of thousands of clients. Here are their top tips.

Top management commitment is key to making implementation of ISO/IEC 27001 a success. They need to be actively involved and approve the resources required.

"The earlier that organizations talk to senior managers, the better it will go for them so have those discussions early."
John Scott, Overbury, leading UK fit-out and refurbishment business

Think about how **different departments work together** to avoid silos. Make sure the organization works as a team for the benefit of customers and the organization.

"The key to implementing the standard lies in getting staff to think about information security as an integral part of the daily business and not as an additional burden."
Mr. Thamer, Ibrahim Ali Arab, Assistant General Manager IT

Review systems, policies, procedures and processes you have in place – you may already do much of what's in the standard – and make it work for your business. You shouldn't be doing something just for the sake of the standard.

"Don't try and change your business to fit the standard. Think about how you do things and how that standard reflects on how you do it, rather than the other way around."
Paul Brazier, Commercial Director, Overbury

Speak to your customers and suppliers. They may be able to suggest improvements and give feedback on your service.

"This certification allows us to go one step further by offering our customers the peace of mind that we have the best controls in place to identify and reduce any risks to confidential information."
Jitesh Bavisi, Director of Compliance, Exponential-eBavisi

Train your staff to carry our internal audits of the system. This can help with their understanding, but it could also provide valuable feedback on potential problems or opportunities for achievement.

"The course was loaded with practical exercises and real-case scenarios and was structured in a way that it encouraged participants to be interactive and share their experiences in information security."
Nataliya Stephenson Manager, Information Security, NSW Attorney General's Department

And finally, when you gain certification, celebrate your achievement and use the **BSI Assurance Mark** on your literature, website and promotional material.

bsi.
ISO/IEC 27001:2013
Information Security Management

5. Your **ISO/IEC 27001** journey.

Whether you're new to information security management or looking to enhance your current system, we have the right resources and training courses to help you understand and implement ISO/IEC 27001. We can help make sure your system keeps on delivering the best for your business.

	You need to:	We help you:
Understand and prepare	• Buy the standard and read it; understand the content, your requirements and how it will improve your business • Contact us; we can propose a solution tailored to your organization's needs	• Discover information on our website, including case studies, whitepapers and webinars visit **bsiamerica.com** • BSI ISO/IEC 27001:2013 Requirements training
See how ready you are	• Ensure your organization understands the principles of ISO/IEC 27001 and the roles individuals will need to play. Review your activities and processes against the standard	• Download self-assessment checklist • BSI ISO 27001:2013 Implementation training course • Schedule a BSI gap assessment to see where you are • BSI Business Improvement Software can support ISO/IEC 27001 implementation
Review and get certified	• Contact us to schedule your certification assessment • We will then carry out system and document assessments (a 2 stage process). The length of this may depend of the size of your organization	• BSI ISO/IEC 27001:2013 Internal and Lead Auditor training • BSI Business Improvement Software helps ISO/IEC 27001 implementation • Your BSI certification assessment

Continually improve and make excellence a habit

Your journey doesn't stop with certification. We can help you to fine-tune your organization so it performs at its best.

- Celebrate and promote your success – download and use the BSI Assurance Mark to show you are certified.
- BSI ISO/IEC 27001 Lead Auditor qualification can help advance your auditing skills.
- BSI Business Improvement Software will help you to manage systems and drive performance.
- Your BSI Client Manager will visit you regularly to make sure you remain compliant and support your continual improvement.
- Consider integrating other management system standards to maximize business benefits.

Your implementation guide to **ISO/IEC 27001**

6. BSI Training Academy

Boost your knowledge with our expertise: BSI has a comprehensive range of training courses to support implementation of ISO/IEC 27001 and helps build the skills in your organization. Our expert instructors can transfer the knowledge, skills and tools your people need to embed the standards of excellence into your organization. What's more, the accelerated learning techniques applied in our courses will help make sure that what you learn stays with you.

Courses that help you understand ISO/IEC 27001 include:

BSI ISO/IEC 27001:2013 Requirements (TPECS)

- 2-day classroom-based training course
- Learn about the structure and key requirements of ISO/IEC 27001:2013
- Essential for anyone involved in the planning, implementing, maintaining, supervising or auditing of an ISO/IEC 27001:2013 ISMS

BSI ISO/IEC 27001:2013 Implementation

- 2 day classroom-based training course
- Discover the stages of implementation and how to apply a typical framework for implementing ISO/IEC 27001
- Recommended for anyone involved in planning, implementing, maintaining, supervising or auditing of an ISO/IEC 27001 ISMS

ISO/IEC 27001:2013 Lead Implementer

- 5 day classroom-based training course
- Learn and understand the tools and methodologies to lead an ISO/IEC 27001 implementation
- Recommended for anyone involved in planning, implementing, maintaining, supervising or auditing of an ISO/IEC 27001 ISMS

ISO/IEC 27001:2013 Internal Auditor (TPECS)

- 3 day classroom-based training course
- Learn how to initiate an audit, prepare and conduct audit activities, compile and distribute audit reports and complete follow-up activities
- Ideal for anyone involved in auditing, maintaining or supervising an ISO/IEC 27001:2013 ISMS

ISO/IEC 27001:2013 Lead Auditor (TPECS)

- 4 day classroom-based training course
- Gain the skills and understanding required to lead and successfully undertake a successful management system audit
- Recommended for anyone involved in auditing maintaining or supervising an ISO/IEC 27001:2013 ISMS

7. BSI Business Improvement Software

Accelerate implementation time and deliver continual improvements

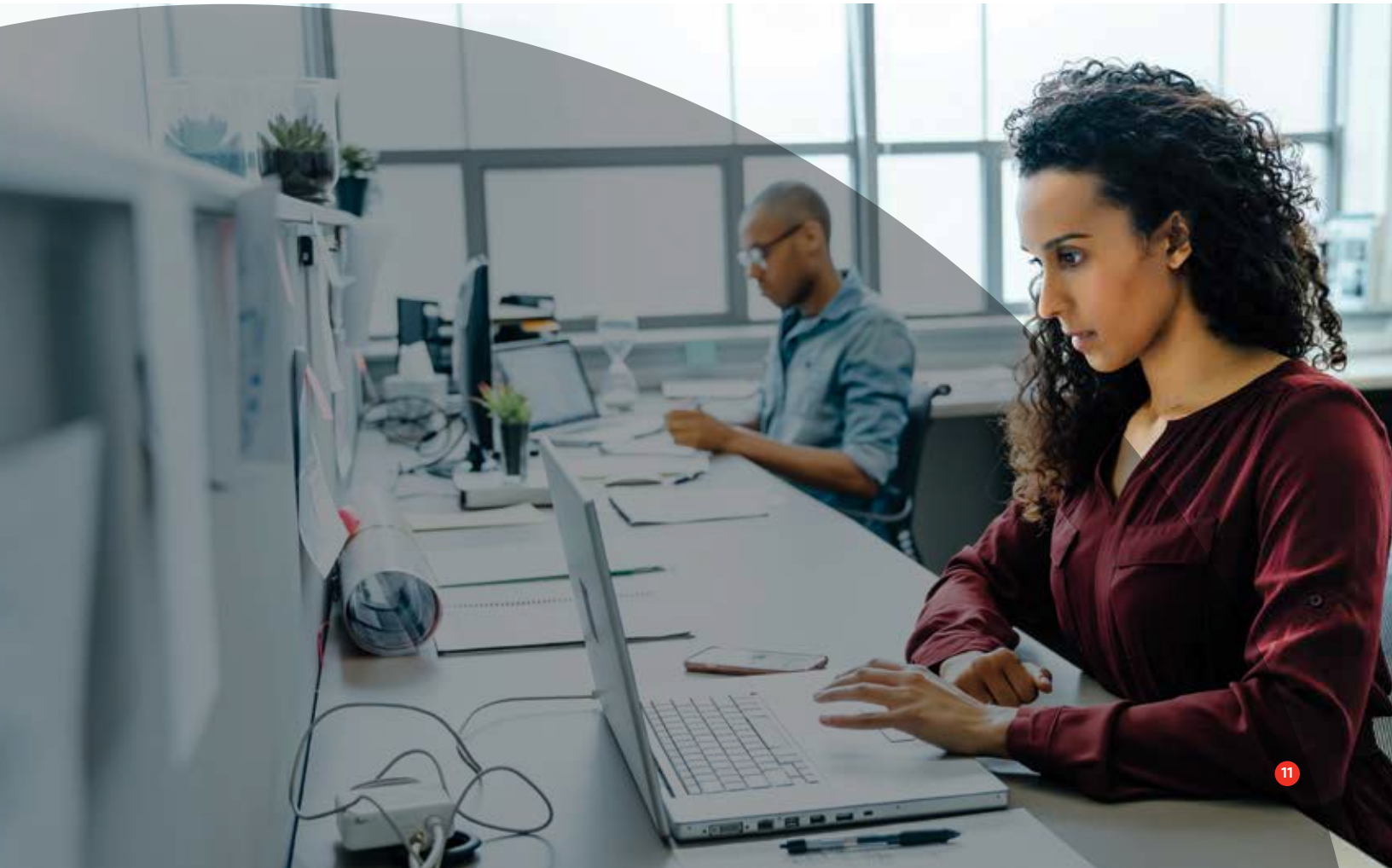
The decision to implement a new management system standard is a huge opportunity to drive business improvement, but initiating, implementing and maintaining this can also be a challenge. Ensuring you get the most from your investment is a key driver to your future success.

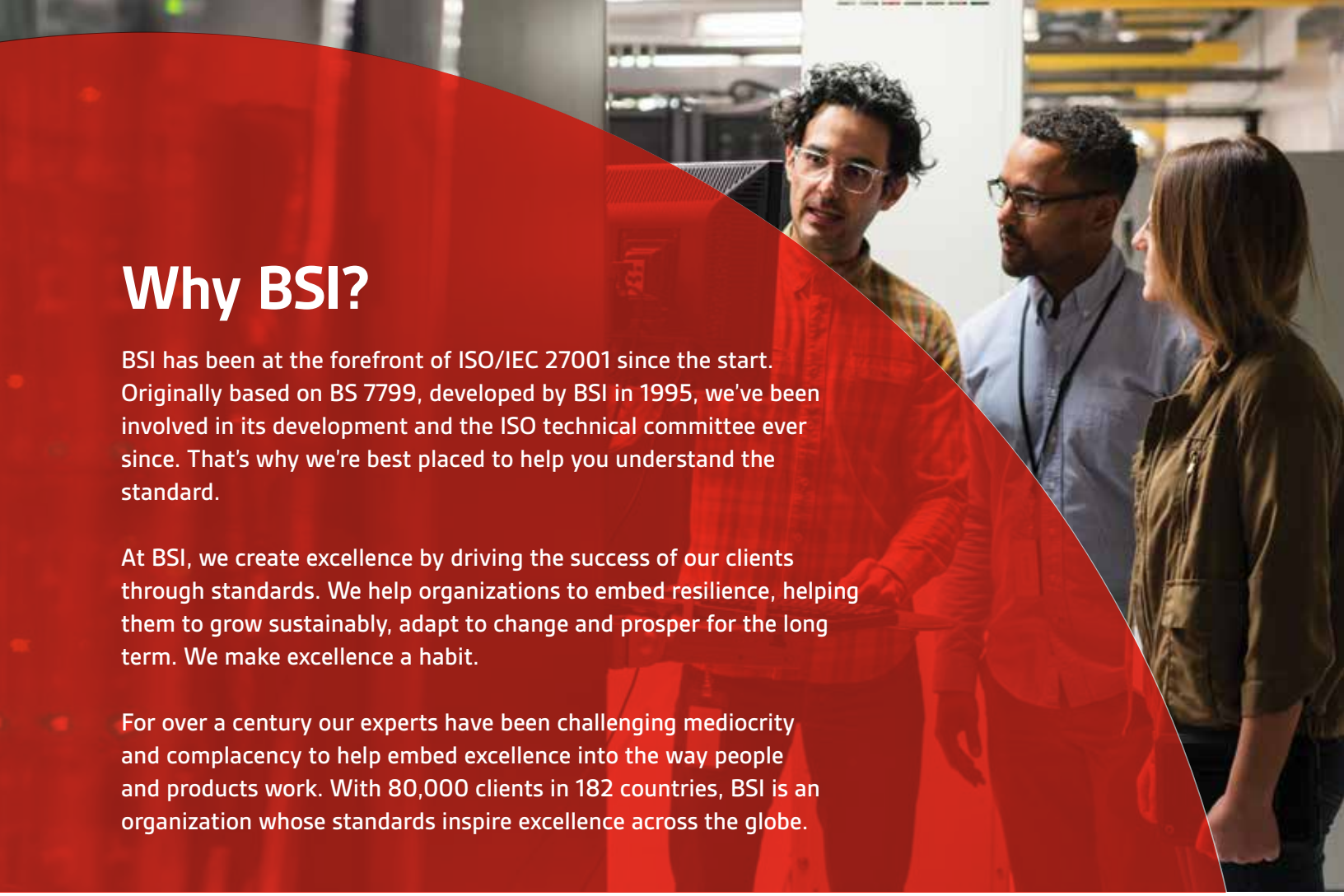
BSI business improvement software provides a solution that can significantly reduce the cost and effort to implement an effective management system, such as ISO/IEC 27001. It can be configured to the requirements of ISO/IEC 27001 and provide your organization with the tools necessary to manage essential elements of ISO/IEC 27001 across your organization. The start of your ISO/IEC 27001 journey is an ideal time to implement BSI business improvement software and sustain the standard successfully.

It can help you to:

- Accelerate implementation time by up to 50%
- Manage your document control effectively
- Provide company-wide visibility on implementation of the standard, so you know exactly where you are at any one time
- Easily and accurately input actions related to audits, incidents/events, risk and performance
- Gain early insight through its customizable dashboards and reporting tools and allow you to quickly see the trends that can help you make business decisions early on and drive improvement

The savings are the costs you avoid because you could not see what was happening at the facility level.





Why BSI?

BSI has been at the forefront of ISO/IEC 27001 since the start. Originally based on BS 7799, developed by BSI in 1995, we've been involved in its development and the ISO technical committee ever since. That's why we're best placed to help you understand the standard.

At BSI, we create excellence by driving the success of our clients through standards. We help organizations to embed resilience, helping them to grow sustainably, adapt to change and prosper for the long term. We make excellence a habit.

For over a century our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work. With 80,000 clients in 182 countries, BSI is an organization whose standards inspire excellence across the globe.

Our product and services

We provide a unique combination of complementary products and services, managed through our three business streams: Knowledge, Assurance and Compliance.

Knowledge

The core of our business centers on the knowledge that we create and impart to our clients. In the standards arena, we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top 10 management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of our standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard, so that it becomes an embedded habit. We provide consultancy services and differentiated management tools to facilitate this process.

By Royal Charter

bsi. ISO/IEC 27001:2013 Information Security Management

bsi.

Find out more
Call 1 800 862 4977
Email inquiry.msamericas@bsigroup.com
bsigroup.com/en-us