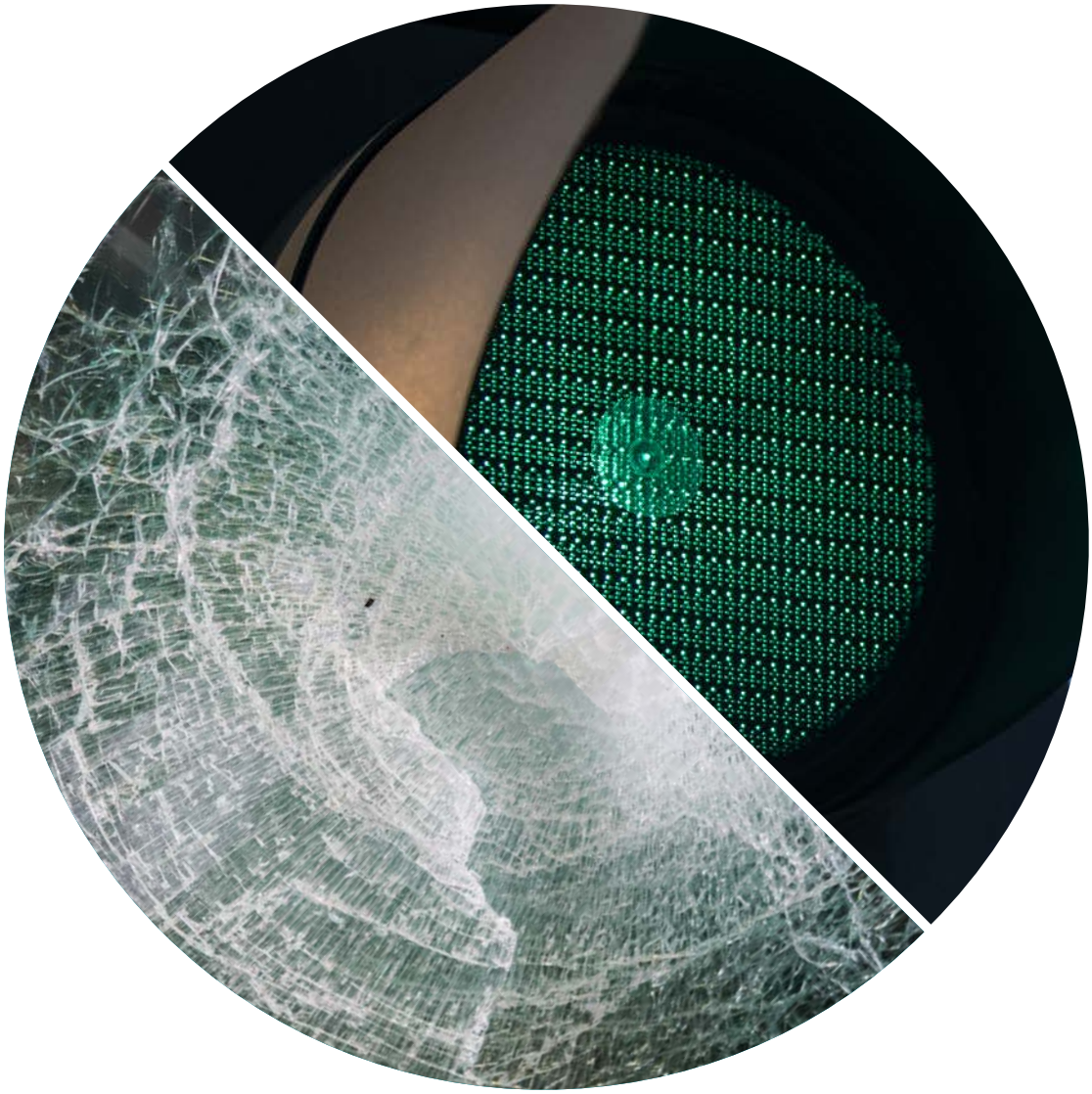
ISO 22301
Business Continuity Management

Your implementation guide



bsi.

...making excellence a habit.™

Build a robust and resilient organization with **ISO 22301**

It's never been more important to protect your business from the unexpected. Whether this is from power cuts, IT system or equipment failure, industrial action, or natural disaster, you need to make sure your business is not vulnerable to disruption and you can recover as quickly as possible.

Statistics indicate that 80% of organisations that are faced with a significant business discontinuity, and do not have in place adequate and appropriate plans to ensure business continuity, do not survive the event. Don't let this happen to you.

At BSI we have the experience to help make sure you get the most from **ISO 22301**. In fact it was our experts who helped shape its precursor, BS 25999-2, in the first place.

This guide shows you how to implement **ISO 22301,** and helps you put in place the measures to protect your business and help it thrive for the long term. We also showcase our additional support services, which help you to not only achieve certification, but also help you to continually improve your business.

"A disaster can strike an organization at any time. You need to have a process in place that ensures the operation is able to mitigate the impact and return to "business as usual" as quickly as possible. For us at Vauxhall ISO 22301 fulfills this critical business need."

Phil Millward, GMUK HR Director with overall responsibility to the Board for the BCMS

Contents

How **ISO 22301** works and what it delivers for you and your company

ISO 22301 is the international standard that helps organizations put business continuity plans in place to protect them, and help them recover from, disruptive incidents when they happen. It also helps you to identify potential threats to your business and to build the capacity to deal with unforeseen events.

It helps you to protect your business and your reputation, stay agile and resilient, and to minimize the impact of unexpected interruptions. Whether your business is large or small, the ability to respond quickly and effectively to the unexpected is the key to the survival of any organization. This is why having a robust business continuity management system in place, such as **ISO 22301**, can be considered as one of the most comprehensive approaches to organizational resilience.

Benefits of ISO 22301*

72%
helps protect our business

82%
helps manage business risk

73%
gives trust in our business

56%
increases our competitive edge

"We recognize [ISO 22301] as part of our overall management of strategic and operational risks, nurturing and enhancing our resilience capability and culture."

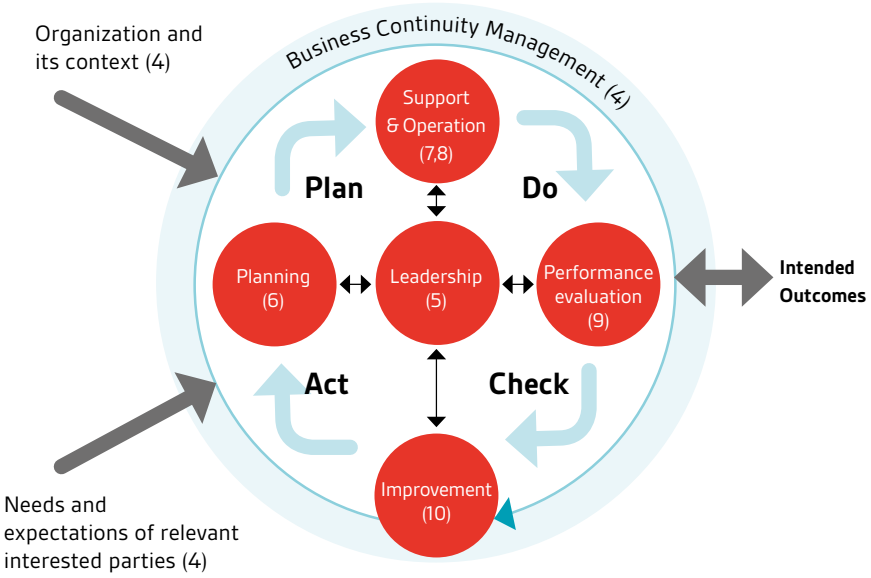
Sanjay Verma, Head of Information Security & Compliance, D&B (Australia)

*Source: BSI Benefits survey - BSI clients were asked which benefits they obtained from ISO 22301

How **ISO 22301** works

ISO 22301 is based on the high level structure (Annex SL) which is a common framework for all new management system standards. This helps keep consistency, align different management system standards, offer matching sub-clauses against the top-level structure and apply common language across all standards. It makes it easier for organizations to incorporate their Business Continuity Management System (BCMS), into core business processes, make efficiencies, and get more involvement from senior management.

Plan-Do-Check-Act (PDCA) is the operating principle of ISO 22301. It's applied to all processes and the BCMS as a whole for continuous improvement. This diagram shows how Clauses 4 to 10 of ISO 22301 can be grouped in relation to PDCA.



Some of the core concepts of ISO 22301 are:

Concept	Comment
Context of the organization	The environment in which the organization operates including internal and external factors that can have an effect on your business continuity plans.
Interested parties	A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. Examples include suppliers, customers or competitors. You may refer to them as stakeholders.
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.
Performance evaluation	The measurement of performance and effectiveness of the BCMS, covering the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results.
Maximum Acceptable Outage (MAO)	The time it would take for adverse impacts to become unacceptable. This is the same as 'maximum tolerable period of disruption (MTPD)'.
Minimum Business Continuity Objective (MBCO)	The minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.
Prioritized timeframes	Order and timing of recovery for critical activities.
Warning and communication	Activities undertaken during an incident.

Key requirements of ISO 22301

Clause 1: Scope

The first clause details the scope of the standard.

Clause 2: Normative references

This clause provides the normative references contained in the standard.

Clause 3: Terms and definitions

Please refer to the terms and definitions contained in ISO 22300. This is an important document to read.

Clause 4: Context of the organization

This clause is a good starting point to approach the standard as you need to decide on the context of your BCMS and how your organizations' strategy supports this. This means that you need to identify how your organization sits within its environment.

You will need to identify external and internal issues that are relevant to the purpose of the BCMS and how they relate to its expected outcomes.

Then you'll need to identify your relevant internal and external "interested parties" (or stakeholders) who are relevant to the BCMS.

You'll also need to decide what is covered by business continuity and just as importantly what isn't. This means that you will need to consider your appetite for risk and what the relevant legal and regulatory requirements for your organization are.

You will be required to communicate this scope to relevant interested parties both internally and externally so they are aware of your BCMS and how it is relevant to them.

Clause 5: Leadership

This clause focuses on the role and requirements of top management, which is the group of people who direct and control your organization at the highest level in relation to the BCMS.

Top management must show their commitment to the BCMS in a number of different ways. Firstly, by ensuring the BCMS is compatible with the strategic direction of the organization. Secondly, they need to show how your BCMS requirements are integrated into your business processes. And lastly by communicating the importance of an effective BCMS and conforming to the BCMS requirements.

Policy creation and communication is a really important part of this clause. You will need to ensure that your business continuity policy is appropriate for your organization and that it meets relevant legal and regulatory requirements. It should also be made available to all interested parties you have identified.

Top management should assign responsibility for the establishment, implementation and monitoring of the BCMS. And finally, you will also need to show how you continually improve the BCMS.

Clause 6: Planning

This clause relates to establishing the strategic objectives and guiding principles of the BCMS as a whole. It requires you to consider the risks from your BCMS not being successfully implemented.

This means that you need to make sure you understand both the internal culture and the external environment in which your organization operates and also what the likely barriers may be in preventing your BCMS from being effective.

You will be required to clearly define your business continuity objectives and show that you have plans to achieve them. Your objectives should be measureable.

You will also need to decide on the minimum level of products and services that will be acceptable to your organization in order to achieve your business objectives. (This links back to the scope that you have defined in clause 1).

You'll need to decide who will be responsible for delivering the objectives, what will be done in what timescale, what resources will be required, and how the results will be evaluated.

Clause 7: Support

This clause is all about the resources that are required to establish, implement and maintain an effective BCMS. You'll need to make sure that people are competent in terms of education, training, awareness and experience. You will also need to consider the communications with interested parties and your requirements for document management.

Taking into consideration the increased use of subcontractors in today's business environment this clause requires you to make sure that everyone under the control of your BCMS understands their contribution to its effectiveness and the implications of not conforming to it. Critically, they must understand their role at the time of a disruption. You will also need to show how you respond to communications from interested parties.

It is crucial that your organization fully documents all elements of the BCMS and these documents must be maintained, controlled, and stored appropriately. (How you do this is up to you, but it must be effective for your organization).

Clause 8: Operation

In this clause you must show how the processes that you have developed to manage the risks to the BCMS are being correctly implemented. This includes any processes that may have been subcontracted or outsourced.

You need to define the order and timing of recovery for critical activities that support your organizations products and services. This includes deciding on what a minimum acceptable level is.

You need to be aware that there may be certain financial or governmental obligations that require communication and that there may be a societal need to share certain information in the event of a disruption. Your process should focus on minimizing the consequences of a disruption.

You will also need to have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident.

Although you do not need to have an approved exercise programme in place to check the effectiveness of your BCMS, you do need to have exercises based on an appropriate range of scenarios. Lastly, you will need to promote continual improvement of the BCMS.

Clause 9: Performance evaluation

This clause covers the maintaining and reviewing of the BCMS so it is kept relevant and up-to-date. This is so that you have the metrics in place to ensure that you effectively manage the BCMS and continually improve.

After an internal audit, the management responsible for the area being audited must ensure that any corrections or corrective actions that have been identified are carried out without delay.

This clause also covers management review. You will need to provide information for review on the trends in; nonconformities and corrective actions, monitoring and measurement evaluation results, and auditing results.

Finally, there is a requirement for your organization to communicate the results of the management review to relevant interested parties and take appropriate actions relating to those results.

Clause 10: Improvement

This clause is all about making your BCMS as effective as it can be to show how you are proactive in managing it.

You are required to show how you continually improve and enhance the performance of your BCMS to ensure it is robust and relevant. This may be, as a result of identifying potential threats or risks from any internal or external factors that are relevant to your organization.

You will also need to show how the BCMS has been updated in response to any non-conformities or corrective actions.

Top tips on making **ISO 22301** effective for you

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

Top management commitment is key to making this a success

"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

Keep staff informed of what's going on, create a team or assign a champion, as this will increase motivation. This could include a well communicated plan of activities and timescales.

"When we decided to implement the new standard, we assigned an internal champion of the standard inside the organization".

Ronald Tse, Ribose, Hong Kong based cloud services provider

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.

"With ISO 22301 in place, we are all talking the same language about the business. We all understand what is meant by best practices and we are better able to deliver on our customers' expectations even during an impactful business event".

Dan Nickel, Ciena, US based network solutions provider

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.

"The BCM system is a great reassurance. It has enabled us to make plans to mitigate problems quickly if they occur– for example, to identify a second water supply and provide electricity back-up – things we wouldn't have done otherwise".

Andy Drummond, Lettergold Plastics Ltd, UK engineering company

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

"They [customers] know we have a solid framework for service continuity and ability to restore all services to business as usual operation in the least possible time".

Sanjay Verma, Dunn & Bradstreet (Australia), global business information provider

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.

"Staff awareness training was vital to the success of ISO 22301 implementation project".

Jide Orimolade, AIICO Insurance, Nigerian life insurance provider

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

Your **ISO 22301** Journey

Whether you are new to business continuity management or looking to enhance your current system, we have the right resources and training courses to help you implement ISO 22301. But our support doesn't stop there. 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, understand the content, your requirements and how it will help and protect your business • Contact us for a proposal tailored to your organizations needs	• Buy the standard • Discover information on our website, including case studies, whitepapers and webinars visit **bsigroup.com** • Attend a BSI ISO 22301 Requirements training course
See how ready you are	• Ensure your organization understands the principles of ISO 22301, the roles individuals in your business will need to play and review your activities and processes against the standard	• Download the self-assessment checklist • Attend a BSI Implementing ISO 22301 training course • Book a BSI gap assessment to see where you are • BSI Business Improvement Software can support your ISO 22301 implementation
Review and get certified	• Contact us to book your certification assessment • Ensure the right people are available for your audit visit(s). This is a two-stage process. The length varies depending on the size of your organization	• Attend a BSI ISO 22301 Internal or Lead Auditor training course • BSI Business Improvement Software can help your ISO 22301 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.
- Book any of our additional Business Continuity training courses which can further your knowledge.
- Use BSI Business Improvement Software to help you 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.

BSI Training Academy

The BSI Training Academy is a world leader in helping clients develop the knowledge and skills they need to embed excellence in their organizations. We offer a range of ISO 22301 training solutions that can be tailored to your needs. Our training courses are developed by experts in their fields who have been directly involved in the development of ISO 22301, so when you train with us you'll benefit from their expertise.

Using the latest research, our accelerated learning approach is proven to fast-track learning and improve knowledge retention. Our experienced tutors can help you get to grips with the matters that concern you and your organization directly, whether delivered in-house or as part of an open course where other delegates can share their experience.

Courses that help you understand ISO 22301 include:

ISO 22301 Requirements

- One-day classroom-based training course
- Learn about the structure and key requirements of ISO 22301
- Essential for anyone involved in the planning, implementing, maintaining, supervising or auditing of an ISO 22301 BCMS

ISO 22301 Implementation

- Three-day classroom based training course
- Discover how to apply a typical framework for implementing ISO 22301 following the PDCA cycle and using the handy resources contained in the good practice toolkit
- Recommended for anyone involved in the planning, implementing, maintaining, supervising or auditing of an ISO 22301 BCMS

ISO 22301 Internal Auditor

- Two-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 22301 BCMS

ISO 22301 Lead Auditor

- Five-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 22301 BCMS.

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 22301. It can be configured to the requirements of ISO 22301 and provide your organization with the tools necessary to manage essential elements of ISO 22301 across your organization. The start of your ISO 22301 journey is an ideal time to implement BSI business improvement software to support your BCMS.

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
- You can easily and accurately input actions related to audits, incidents/events, risk and performance
- Through its customizable dashboards and reporting tools it gives you early insight into trends that 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?

By Royal Charter

bsi. ISO 22301 Business Continuity Management

BSI has been at the forefront of ISO 22301 since the original Business Continuity Standard, BS 25999-2 was pioneered by us in 2007. And we continue to be at the forefront of developing and evolving standards to keep organizations resilient and robust. 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 products 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 centres 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 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.

bsi.

Find out more
Call: +6 03 2242 4211
Visit: bsigroup.com.my