Strengthening Resilience with Business Continuity Management ISO 22301

Your implementation guide

Business continuity that drives competitive advantage

Minimize the impact of disruptive incidents with ISO 22301, the international standard for business continuity management.

An effective business continuity management system (BCMS) built on and certified to ISO 22301, can empower you in the face of disruption. It enables you to respond to an incident in a measured way and return quickly to business as usual. By following international best practice set out in ISO 22301, you can also strengthen compliance measures and reduce uncertainty after an incident occurs.

Implementing and certifying to ISO 22301 can be far more than a defensive measure. It can be a strategic investment that transforms your BCMS, turning it into a valuable asset. Leveraging this internationally recognized standard enables you to foster trust and gain a competitive advantage by showing customers, partners, and stakeholders that you not only

prioritize business as usual but have measured control over your operations.

ISO 22301 also helps you ensure you are as efficient as possible by providing you with the framework and knowledge to implement the correct solutions and scale specific to your organization. By understanding the maximum acceptable disruption clients will accept for a particular service, you can ensure resources are allocated appropriately and avoid overextending.

- Business continuity and resilience professionals now rate their role as more strategic than operational.

- 75% of organizations ensure the ultimate responsibility for resilience lies within the C-suite[1].

"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."

HR Director, Automotive Industry

[1]BCI Operational Resilience Report 2023, The Business Continuity Institute, BCI Operational Resilience Report 2023 – The BCI, August 2023

Contents

What ISO 22301 delivers for you and your company

ISO 22301 is the international standard that helps you put business continuity plans in place whether your business is large or small. Implementing and certifying to it enables you to:

- Protect your organization and reputation.

- Identify potential threats to your business.

- Recover from disruptive incidents when they happen.

- Minimize the impact of unexpected interruptions.

- Build capacity to deal with unforeseen events.

- Stay agile and resilient going forward.

- Demonstrate control over business operations to customers and stakeholders.

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

Information Security & Compliance Head,
Commercial Data Provider

How ISO 22301 works

ISO 22301 is based on the ISO harmonized approach, 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 also makes it easier for organizations to incorporate their BCMS into core business processes, make efficiencies, and get more involvement from senior management.

The operating principle of ISO 22301 is Plan-Do-Check-Act (PDCA), 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.
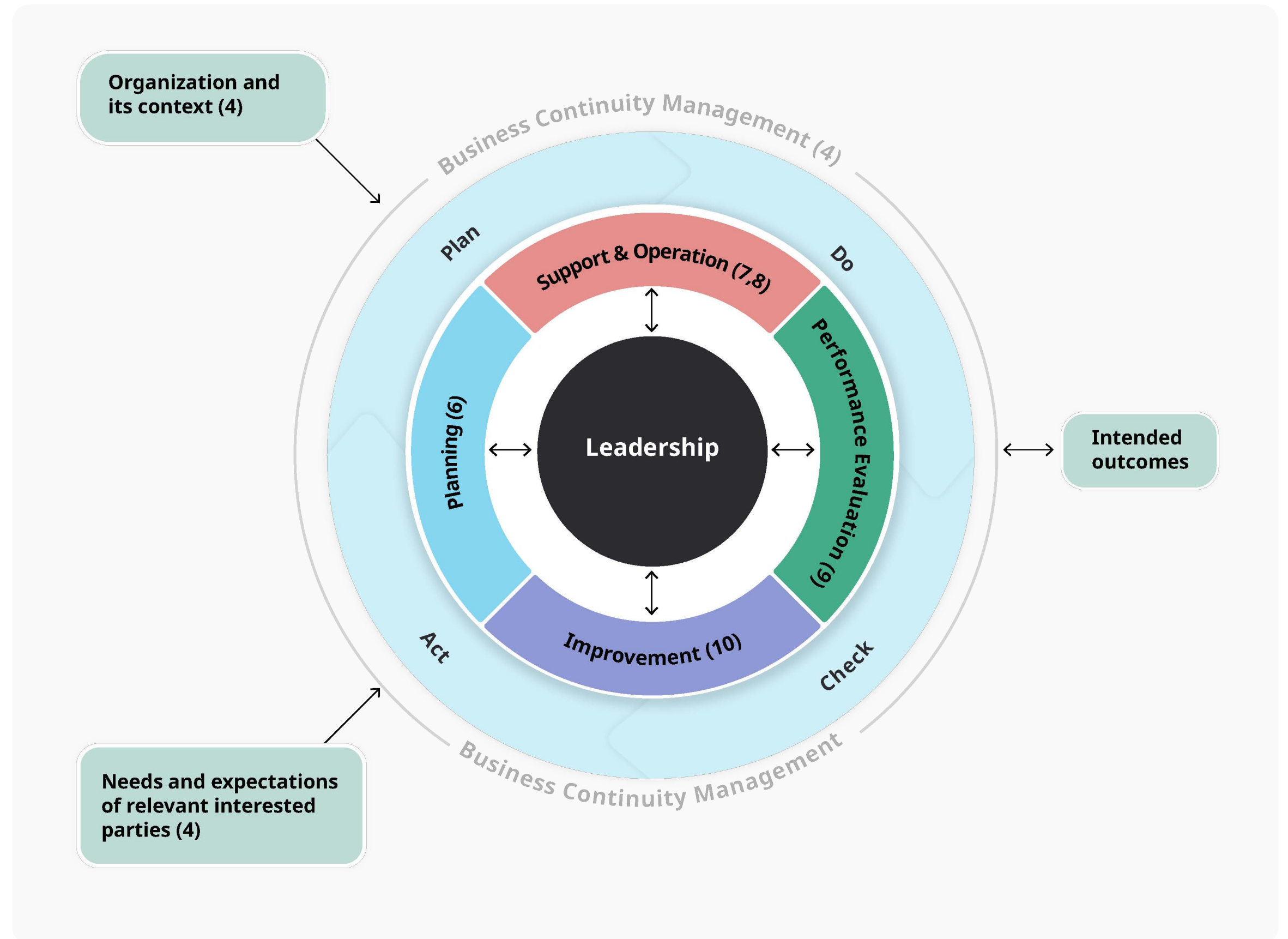
Some of the core concepts of ISO 22301 are:

Context of the organization
The environment in which your organization operates. This includes internal and external factors that can affect 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. This covers the applicable methods for monitoring, measurement, analysis and evaluation to ensure valid results.
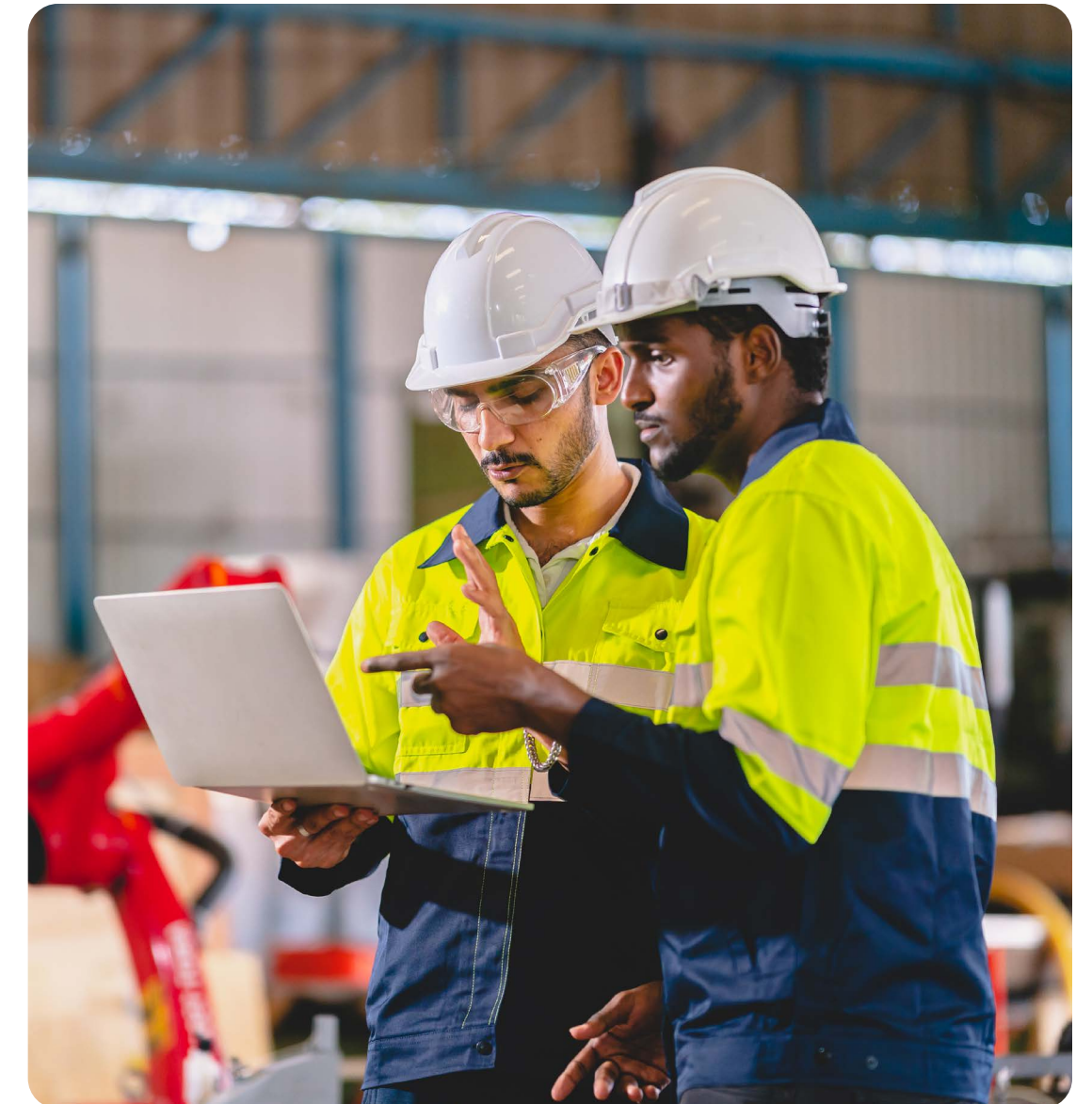
Some of the core concepts of ISO 22301 are:

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

Detailing the scope of the standard.

Clause 2:
Normative references

Providing the normative references contained in the standard.

Clause 3:
Terms and definitions

This clause provides cross-reference to the terms and conditions contained in ISO 22300 (Security and resilience).

Clause 4:
Context of the organization

This provides a good starting point to approach the standard as you need to decide on the context of your BCMS and how your organization's strategy supports this. This means 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 you will need to consider your appetite for risk and what the relevant legal and regulatory requirements are for your organization.

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 focuses on the role and requirements of top management, 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 several different ways. The first is 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. Lastly, they need to communicate the importance of an effective BCMS and of 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 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

Establishing the strategic objectives and guiding principles of the BCMS as a whole, this clause requires you to consider the risks from your BCMS not being successfully implemented.

You need to ensure you understand your organization's internal culture and external environment and the likely barriers 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 measurable.

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

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

Clause 7:

Support

This clause requires you to identify and understand the resources 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.

This clause requires you to make sure everyone under the control of your BCMS understands their contribution to its effectiveness and the implications of not conforming. This includes subcontractors, who are increasingly being used in today's business environment. Critically, each person 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 that 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 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 organization's 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 also 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.

You do not need to have an approved exercise programme in place to check the effectiveness of your BCMS. But 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 you have the metrics in place to ensure 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, your organization must 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 possible to show how you are proactive in managing it. You must 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 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

Our clients shared their top tips on how to make ISO 22301 implementation and certification as seamless as possible.

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".

Director, Technology 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 backup – things we wouldn't have done otherwise".

Owner, Chemical Manufacturing.

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".

CEO, Technology Provider.

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".

Head of Information Security & Compliance, Global Business Information Provider.

Train your staff to carry out 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".

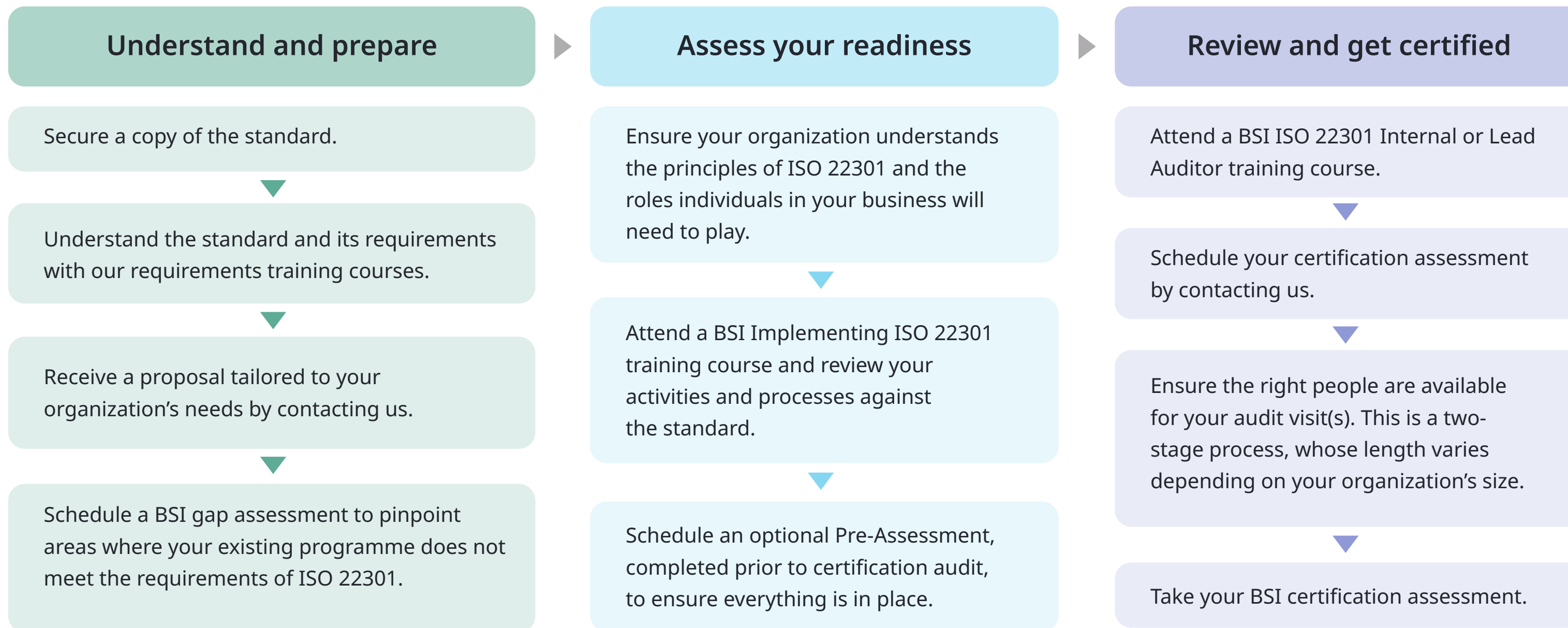**Chief Executive**, Life Insurance Provider.

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".

Group Health & Safety Manager, Construction Services.

Starting your ISO 22301 Journey

Whether you're new to business continuity management or want to enhance your current system, we can help. Our resources, training courses, and expertise will help you implement and optimize your ISO 22301 BCMS via the following steps:

Understand and prepare

Secure a copy of the standard.

▼

Understand the standard and its requirements with our requirements training courses.

▼

Receive a proposal tailored to your organization's needs by contacting us.

▼

Schedule a BSI gap assessment to pinpoint areas where your existing programme does not meet the requirements of ISO 22301.

Assess your readiness

Ensure your organization understands the principles of ISO 22301 and the roles individuals in your business will need to play.

▼

Attend a BSI Implementing ISO 22301 training course and review your activities and processes against the standard.

▼

Schedule an optional Pre-Assessment, completed prior to certification audit, to ensure everything is in place.

Review and get certified

Attend a BSI ISO 22301 Internal or Lead Auditor training course.

▼

Schedule your certification assessment by contacting us.

▼

Ensure the right people are available for your audit visit(s). This is a two-stage process, whose length varies depending on your organization's size.

▼

Take your BSI certification assessment.

Continually improve and deliver impact

Your journey doesn't stop with certification. We can help your organization make continuous improvements so it performs at its best.

Celebrate and promote your success – download and use the BSI Assurance Mark on your literature, website and promotional materials to show you are certified.

Book any of our additional business continuity training courses which can further your knowledge.

Use the BSI Connect Portal 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.

Supporting your journey towards certification

Whether you're new to business continuity management or want to enhance your current system, we can help. As your trusted partner, we ensure your system maintains operational resilience, fosters trust, and increases customer trust for a competitive edge.

Understand and prepare with Training and Qualifications

Strengthen your knowledge on what ISO 22301 Business Continuity Management does, how to implement it, and how to audit your system in our range of training courses and professional qualifications. We also offer courses focused on key skills that bolster your abilities and knowledge as a Business Continuity professional, such as a Business Impact Assessment, and Crisis Management.

Discover our courses

Measure your readiness with Pre-Certification Assessments

As an optional early-stage review, a Gap Assessment pinpoints areas where your existing BCMS does not meet the requirements of ISO 22301.

A Pre-Assessment is also highly recommended, completed prior to certification audit to ensure everything is in place.

Identify your BCMS gaps

Getting and maintaining certification

We conduct the formal certification audit to evaluate your BCMS against ISO 22301. This comprehensive review ensures that all aspects of your business continuity plan are compliant and effective. Once you successfully complete the certification audit, BSI awards you with an accredited and international-recognized certification.

Get ISO 22301 certified

Why BSI?

Developing best practice in a fast-moving business landscape

Having been on the frontline of technological progress for more than a century, BSI has been working with organizations across the globe to build trust in digital risk 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.

Backed by technical prowess and a robust network of industry leaders, academics, and professional bodies, BSI is committed to advancing the digital trust agenda.

Partner with us to navigate the complexities of privacy and information security with confidence.

Talk to us about your business continuity requirements

Contact us