

**HOW CAN YOU ENSURE BUSINESS CONTINUITY?
ISO 22301 AUDITS, CERTIFICATION AND TRAINING**

ISO 22301 BUSINESS CONTINUITY MANAGEMENT SYSTEMS

Most organisations will, at some point, be faced with having to respond to an incident which may disrupt or threaten the day-to-day operations of their business. A successful Business Continuity Management (BCM) programme, established to respond to any potential disruption, is essential for all organisations. Ensuring a holistic Business Continuity Management System (BCMS) is in place will not only help your organisation recover from disasters, it will also prevent the reputational damage that can arise from any operational outages, missed deadlines, upset customers, or direct financial loss. Certification against the requirements of ISO 22301, the International standard for Business Continuity Management, enables you to demonstrate your commitment to having a most robust BCMS in place. Partnering with SGS enables you to improve your risk management by implementing effective business continuity management systems, developing increasingly skillful talent and ensuring consistent and compliant supply chains are in place.

INTRODUCTION TO ISO 22301

Business Continuity Management involves the recovery or continuation of business activities in the event of any business disruption. The overall BCM programme must be managed through activities such as scoping, risk evaluation, business continuity strategy, business continuity objectives, development planning, training, exercises, testing, reviewing and continual development. Even if an organisation has never experienced a serious incident, establishing a BCMS, built on ISO 22301, helps to define key business processes and the disruption that could result from any threats.

ISO 22301 provides a comprehensive set of controls based on BCM best practice, covering the whole BCM lifecycle. It defines the strategic and tactical capability of an organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level. The standard is generic and offers organisations guidance on putting their BCM systems in place. An organisation can prepare for the worst and take steps to improve its resilience.

The BCMS should also include Risk Assessment (RA) and Business Impact Analysis (BIA), which are an inherent part of ISO 22301 and an essential component to identifying prioritized activities, dependences and resources supporting their key products and services, as well as what the impact of their failure would be on the organisation.

THE BENEFITS

The ISO 22301 certification will help improve any business by ensuring planned, effective BCM at all levels, including:

- Organisation-wide identification and understanding of critical business processes and the impact of disruption
- Increased levels of resilience and recovery capability, and the continued survival of the organisation
- Advantage gained over less resilient competitors
- Positive message communicated to the media and stakeholders in crisis conditions

- Improved risk profile in the minds of insurers, resulting in reduced insurance premiums
- Compliance with the expectations of regulators, insurers, business partners and other key stakeholders
- Significantly reduced financial impact of incidents, disruption or even under disaster
- Increase the survival chance of both the organization and employees
- Reputation maintained, or even improved, through demonstrating a professional approach to managing disruption
- Timely and orderly responses to incidents and business disruptions to continue business operations at an acceptable pre-defined level as promises in contract or agreement
- Encourages cross-team and cross-organization coordination
- Demonstrate credible responses through scenario-base exercising
- Demonstrate management commitment in overall risk management with visible evidence

HOW ISO 22301 IMPROVES ON BS 25999

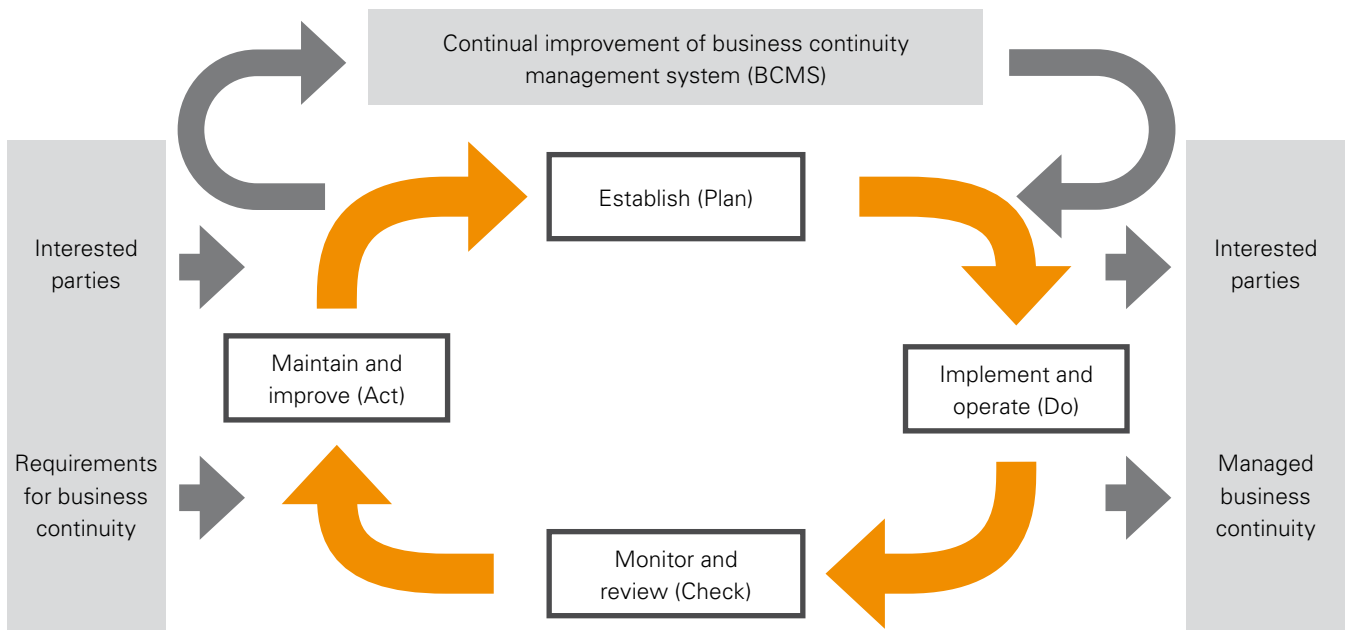
If your organisation has implemented BS 25999 you can take advantage of a short cut upgrade to ISO 22301. To assist with the process, business needs must be logged and executive management must continually refine organisation-wide business continuity policy and objectives to better prepare for ISO 22301 certification.

Cost-benefit analysis should be used to review all business continuity arrangements, such as service level agreements, shared space, workforce, alternative process and technologies during and after the emergency. Regular assessment of overall business continuity capability to manage disruptive incidents is suggested, as is a scheduled series of exercises on an annual basis in line with business priorities and risk exposure. This is designed to highlight any areas of weakness, giving you a better ability to manage all types of potential incidents or disasters.

Awareness, training and continual refreshment are essential for a robust BCMS and ways to continually improve their effectiveness are based on objective measurement such as audit results, test results and feedback from interested parties resulting in a better level of organised response to any unexpected disruptions.



EMBEDDING BCM INTO THE ORGANISATION'S CULTURE



THE BCM PROCESS

The BCM process consists of six steps:

- Step 1 – BCM programme management: Programme management enables the business continuity capability to be both established (if necessary) and maintained in a manner appropriate to the size and complexity of the organisation. Documented approval of BCM scope and authorisation of a core team with BCM roles and responsibilities are key issues to be defined in this first step.
- Step 2 – Understanding the organisation: The activities associated with this step provide the information that enables prioritisation of an organisation's products and services, and identifies critical supporting activities and the resources that are required to deliver them. Business Impact Analysis (BIA) and Risk Assessment are also crucial parts of this stage.
- Step 3 – Determining business continuity management strategies: This allows an appropriate response to be chosen for prioritised business activities so that an organisation can continue and recover their service or product within a pre-defined timeframe after disruption. Pre-defined critical timeframes such as MAO, MBCO, MTPD, RTO and RPO are needed prior to developing the plan.
- Step 4 – Developing and implementing a BCM response: This involves developing emergency response, crisis management and business continuity plans that detail the steps to be taken during and after a disruption to maintain or restore prioritised business processes or operations at a pre-defined level.
- Step 5 – Exercising, maintaining and reviewing BCM arrangements: This allows the organisation to demonstrate the extent to which its strategies and plans are fit for purpose, with exercises at planned intervals to support business continuity objectives and to identify opportunities for improvement.
- Step 6 – Embedding BCM in the organisation's culture: This enables BCM to become part of the organisation's core values and instils confidence in all interested parties in the ability of the organisation to cope with disruptions. Organisations need to train those responsible for implementing BCM and acting in the event of disruption, as well as those who will be impacted by the plans. Organisations should not only put plans in place, but should review them regularly to keep up-to-date and ensure their effectiveness. Organisation can consider integrating multiple management systems to maximise efficiency.

ISO 22301 abbreviations are as follows:

MAO: Maximum Acceptable Outage

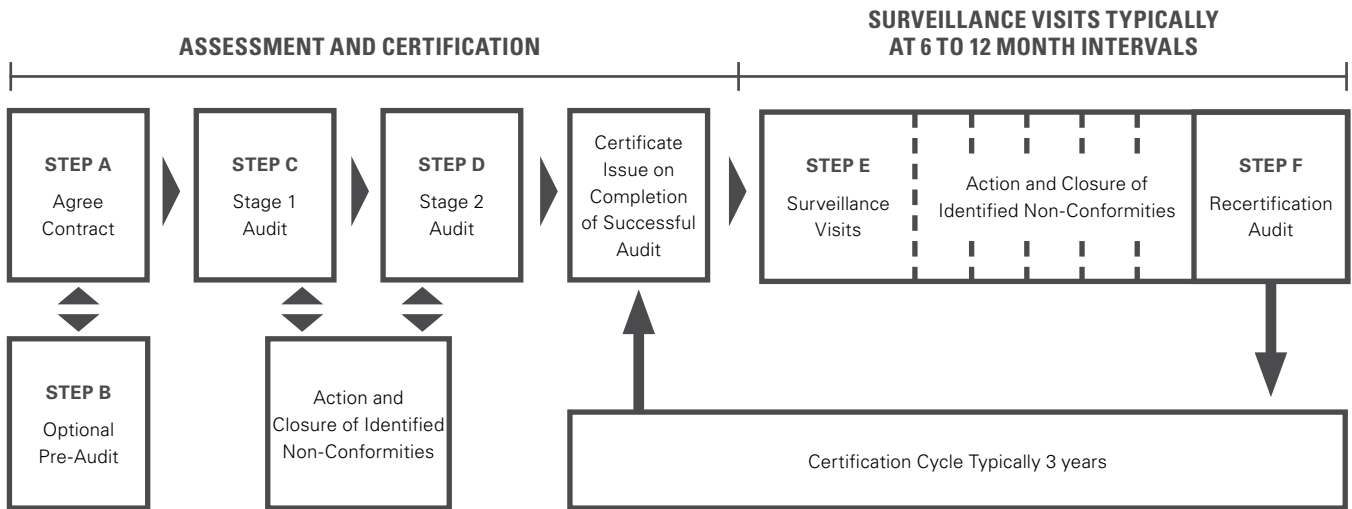
MBCO: Minimum Business Continuity Objective

MTPD: Maximum Tolerable Period of Disruption

RTO: Recovery Time Objective

RPO: Recovery Point Objective

ISO 22301 CERTIFICATION PROCESS



HOW DOES THE CERTIFICATION PROCESS WORK?

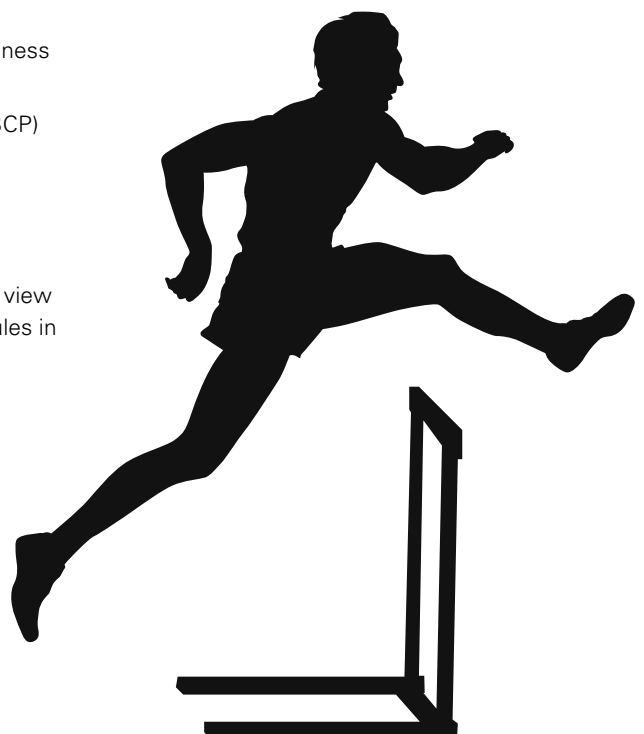
To start the ISO 22301 certification process SGS provides you with a proposal based on the size and nature of your organisation. You may then ask SGS to perform an optional 'pre-audit' to give an indication of your readiness for the formal audit, which starts with a 'Readiness Review'. This evaluates the compliance of your documented system with the requirements of the standard and examines key elements of the system. You will receive a report after this stage identifying any concerns or observed non-compliances. 'Stage Two' of the audit includes staff interviews, the examination of records and the observation of your working practices. We then present the findings, classified as either major or minor non-conformances. Once you have addressed the non-conformities, a technical review will be conducted to confirm the issuance of a certificate. Subsequent visits will be scheduled at either six or 12-month intervals for three years. Then our routine visit will be extended to enable a re-certification audit and visits will continue on a three-year cycle.

ISO 22301 RELATED TRAINING

We offer a wide variety of training courses for all levels of ability and awareness. Our ISO 22301 training course portfolio is designed to meet the requirements of any organisation, and includes:

- BCMS Awareness
- BCMS Architecture and Implementation
- Risk Management and Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- BCMS Internal Auditor
- BCMS Auditor Transition
- BCMS Lead Auditor

Please visit www.sgs.com to view the ISO 22301 course schedules in your region.



**OTHER SERVICES RELATED TO
BUSINESS CONTINUITY
MANAGEMENT SYSTEMS**

SGS is also known for its solutions against other needs related to business continuity management as well as continuous improvement:

- Audit, certification and training related to ISO 31000 (Risk Management), ISO 28000 (Supply Chain Security Management Systems), ISO 27001 (Information Security Management Systems) and to ISO 20000 (IT Service Management Systems)
- Integrated Management Systems: your management systems can be

audited and certified simultaneously with other management systems which you have implemented

- Audit solutions against additional, bespoke quality performance criteria: SGS can help develop the performance criteria and the checklist or simply check performance against existing measures
- Process Improvement solutions leveraging techniques, such as Lean or 5S





WHY SGS?

SGS is the world's leading inspection, verification, testing and certification company. Recognised as the global benchmark for quality and integrity, we employ over 70 000 people and operate a network of more than 1 350 offices and laboratories around the world. We are constantly looking beyond customers' and society's expectations in order to deliver market-leading services wherever they are needed.

SGS is a leading certifying body of Information Security and Business Continuity Management Systems. Partnering with SGS opens the door to better performing processes, increasingly skilful talent, consistent and compliant supply chains and more sustainable customer relationships delivering profitable competitive advantage. Work with the global leader and take your commitment to the next level.

We have a history of undertaking and successfully executing large-scale, complex international projects. With a presence in every single region around the globe, our people speak the language and understand the culture of the local market and operate globally in a consistent, reliable and effective manner.

TO LEARN HOW SGS CAN HELP YOU EXCEED CUSTOMER EXPECTATIONS, VISIT WWW.SGS.COM OR CONTACT CERTIFICATION@SGS.COM FOR MORE INFORMATION.

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

