Transition Guide

Moving from BS 25999-2 to ISO 22301

The new international standard for business continuity management systems

Extract from 'The Route Map to Business Continuity Management: Meeting the Requirements of ISO 22301' by John Sharp

bsi.

...making excellence a habit.™

Successful businesses expect the unexpected and plan for it. Disruptions to your business can result in data risk, revenue loss, failure to deliver services as normal or in extreme cases, failure to deliver at all.

That's why organizations need strong business continuity planning.

This guide has been designed to help you meet the requirements of the new international standard for business continuity management, ISO 22301. ISO 22301 will supersede the original british standard, BS 25999-2 and builds on the success and fundamentals of this standard.

BS ISO 22301 specifies the requirements for setting up and managing an effective business continuity management system (BCMS) for any organization, regardless of type or size. BSI recommends that every business has a system in place to avoid excessive downtime and reduced productivity in the event of an interruption.

Meeting the requirements of the new international standard has never been easier. This guide is an extract from John Sharp's latest book 'The route map to business continuity management' and shares practical guidance on how to meet the requirements of ISO 22301. The book is available through the BSI shop.

This transition guide will help you understand your organization's needs and obligations and how to implement an effective BCMS. Whether you are planning to certify against the new standard or simply want to benefit from BCM best practice, this guide will help you put in place the necessary requirements.

NB: This transition guide is designed to be read in conjunction with BS ISO 22301: 2012 Societal security – Business continuity management systems – Requirements. It does not contain the complete content of the standard and should not be regarded as a primary source of reference in place of the standard itself.

Why adopt a business continuity standard?

As business continuity management (BCM) has developed worldwide, there has been a convergence in the methodologies being promoted. It became apparent following the Year 2000 problem or 'millennium bug', when organizations were deluged with requests for compliance statements from their customers and clients, that there was a need for a uniform approach to BCM.

It is undesirable for major customers to enforce their own approach to BCM down their supply chains, as happened with other management systems, notably quality. While a supplier can run different quality systems to meet the requirements of its customer base, it cannot run different, and possibly conflicting, BCM systems, which will be used during a disruption at a time when tensions are high. This was one of the principal drivers for establishing BCM standards in the UK.

BS 25999 was created to set out a uniform benchmark in good practice, satisfying the needs of customers, clients, government, regulators and all other interested parties. BS 25999 has been accepted worldwide and has formed the basis of many other BCM standards, including the US ASIS/BSI BCM.01 standard adopted by ANSI. BS 25999 and other BCM standards from across the globe provided the source material for the creation of two new international standards: ISO 22301 (requirements) and ISO 22313 (guidance).

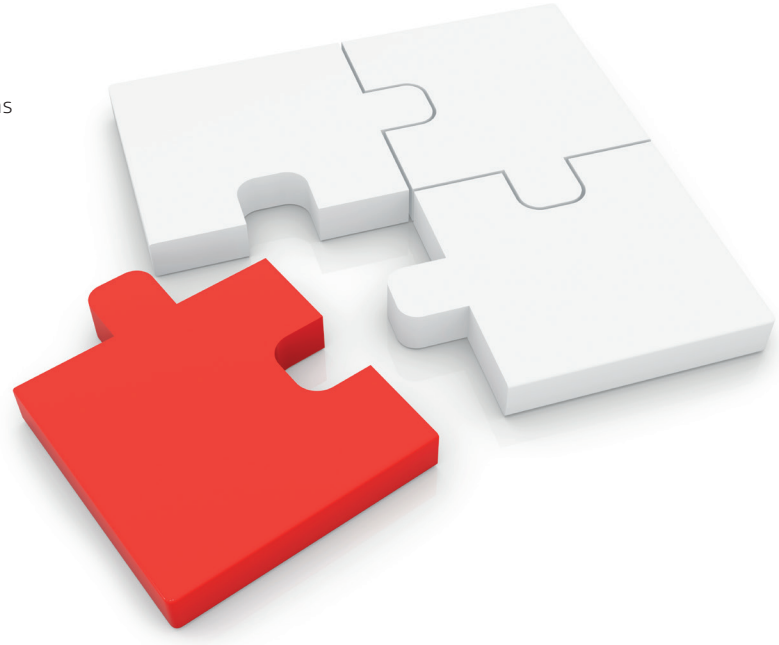
By adopting a standard approach to BCM as set out in ISO 22301, organizations can offer their customers and clients greater assurance that they will be capable of maintaining continuity of operations if they suffer disruptive incidents.

For those already certified to BS 25999-2 there will be a transition period to allow them to update their BCM systems to ISO 22301. For those certified, and those organizations working towards certification, the additional requirements are not onerous.

Implementing ISO 22301

The international standard for BCM, ISO 22301:2012 specifies requirements for setting up and managing an effective business continuity management system (BCMS). It is for use by internal and external parties, including certification bodies, to assess the organization's ability to meet regulatory and customer requirements as well as the organization's own requirements. ISO 22301 contains only those requirements that can be objectively audited and a demonstration of successful implementation can therefore be used by an organization to assure interested parties that an appropriate BCMS is in place.

During the latter part of 2012 or early in 2013, ISO will issue a guidance document ISO 22313. This document will take the form of good practice guidance and recommendations, indicating what practices an organization should, or may, undertake to implement effective BCM. Organizations may choose to follow all or part of the guidance, which may be used for self-assessment or between organizations. The guidance is not a specification for BCM.



Comparing ISO 22301:2012 with BS 25999-2:2007

When news of an ISO standard for BCM emerged, business continuity managers expressed concern that they might have to radically rework their BCM procedures and processes once ISO 22301 was introduced. BS 25999-2 had been, and continues to be, used by many organizations across the world as the basis of their BCM procedures and processes. The good news is that BS 25999-2 has provided the main foundation of the new ISO standard. There are some important additions and a few elements that have been omitted. The additions have added greater depth and clarity while the omissions do not detract from the overall good BCM practices and principles.

The new standard is entitled 'Societal security – Business continuity management systems – Requirements.' This is one of a suite of standards being developed by ISO/TC 223 designed to achieve greater societal security. Societal security can be defined as providing protection of society from, and the ability to respond to, incidents, emergencies and disasters caused by intentional and unintentional human acts, natural hazards, and technical failures.

The way in which ISO 22301 can be used is detailed in Clause 1 Scope. It states that the standard is applicable to all types and sizes of organizations that wish to

- establish, implement, maintain and improve a BCMS
- ensure conformity with stated business continuity policy
- demonstrate conformity to others
- seek certification/registration of its BCMS by an accredited third party certification body
- make a self-determination and self-declaration of conformity with this International Standard [ISO 22301:2012].

The standard can also be used by an organization to assess its suppliers' ability to meet continuity needs and obligations.

New concepts and activities have been introduced as follows.

New Concept	Explanation
Context of the organization	The environment in which the organization operates.
Interested parties	Replaces 'stakeholders'.
Leadership	Requirements specific to top management.
Maximum Acceptable Outage (MAO)	'Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable'. This is the same as 'maximum tolerable period of disruption (MTPD)'.
Minimum Business Continuity Objective (MBCO)	'Minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption'
Performance evaluation	Covers the measurement of BCMS and BCM effectiveness.
Prioritized timeframes	Order and timing of recovery for critical activities.
Warning and communication	Activities undertaken during an incident.

There have been many other additions and some slight alterations to the terms and definitions listed in the standard. The additions and changes reflect terms and definitions commonly used by BCM practitioners today.

The major additions to ISO 22301:2012

Clause 4: Context of the organization

This clause introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements and scope. ISO 22301 requires an organization to 'determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its BCMS'. Understanding the organization and how it sits within its environment is an essential step to ensure any BCMS and BCM solutions developed are fit for purpose and relevant to the organization and interested parties.

This clause also requires the organization to determine its risk appetite and the legal and regulatory requirements that apply to the organization, and to clearly define the scope of the BCMS. Setting the initial scope of the BCMS is critical and must be done at an early stage. ISO 22301 requires the organization to determine what will be covered by business continuity and, just as importantly, what will be excluded. Scoping has presented challenges to many organizations seeking certification under BS 25999-2. Organizations are now required to clearly communicate the scope to relevant internal and external parties.

Clause 5: Leadership

Clause 5 summarizes the requirements specific to top management's role in the BCMS, and how they shall articulate their expectations to the organization via a policy statement.

New requirements are placed upon top management to demonstrate its commitment by:

- ensuring the BCMS is compatible with the strategic direction of the organization
- integrating the BCMS requirements into the organization's business processes
- communicating the importance of effective business continuity management and conforming to the BCMS requirements

In addition it must ensure 'that the BCMS achieves its expected outcomes' and that it directs and supports continual improvement.

Policy creation and communication is an important element of Clause 5. It stresses the importance of ensuring the policy is appropriate to the organization, forms the basis for setting BCM objectives, and contains commitments to meeting legal and regulatory requirements and to continual improvement of the BCMS. It also states that the policy shall be available to appropriate interested parties.

Clause 5 requires top management to assign responsibility for the establishment, implementation and monitoring of the BCMS. What is missing is the requirement to appoint a specific sponsor from top management to 'champion' BCM in the organization. This is a regrettable omission as to be successful; a BCMS must be introduced and supported by top management of the organization. Its involvement is required from the outset and its visible ongoing support is essential if BCM is to be taken seriously by the organization as a whole.

Clause 6: Planning

This is a new section and relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The content of Clause 6 differs from establishing risk treatment opportunities stemming from risk assessment, as well as from the business impact analysis (BIA) derived recovery objectives that are covered in Clause 8.

This section requires the organization to address the threats to the BCMS not being successfully established, implemented and maintained. It is about understanding the internal culture and the external environment in which the organization operates and the likely barriers that will prevent the BCMS being effective. It relates back to Clause 4.1, Understanding of the organization and its context, and Clause 4.2, Understanding the needs and expectations of interested parties.

This clause requires the organization to clearly define the business continuity objectives and to have plans (projects) to achieve them. These objectives must tie back to the BCM policy and must be measurable. In setting the objectives account must be taken of the minimum level of products and services that will be acceptable to the organization in order to achieve its business objectives. Although it does not specify which products and services this applies to, it links back to the Scope (Clause 1) where the organization determined what would be covered by the BCMS. In BS 25999-2 these were referred to as the key products and services.

The organization must also determine who will be responsible for delivering the objectives, what will be done and in what timescale, what resources will be required and how results will be evaluated.

Clause 7: Support

Clause 7 details the support required to establish, implement and maintain an effective BCMS. This covers the resources required, the competence of those involved, awareness of, and communications with, interested parties, and requirements for document management.

BS 25999-2 requires a training needs analysis to be carried out to determine the gap between the competence required to fulfil appropriate BCM roles and the capabilities of those assigned to the roles. ISO 22301 does not specifically require such an analysis but does require an organization to ensure such persons are competent on the basis of education, training and experience.

The section covering awareness is more specific in that it requires all persons under the organization's control to be aware of the BCM policy, understand their contribution to the effectiveness of the BCMS and the implications of not conforming to its requirements. They must also understand their role at the time of disruption.

The major addition in Clause 7 covers communication, a vital part of managing any disruption and an area where many organizations fail. Clause 7.4 relates to internal and external communications and covers information about the BCMS and the organization's BCM capabilities before and during a disruption. It also sets out requirements for receiving and responding to communications from interested parties, adapting and integrating warning and informing systems and facilitating structured communications with appropriate authorities. It requires communications systems to be tested. Further requirements are also specified in Clause 8.4.3.

The requirements for BCMS documentation are more specific in ISO 22301:2012. It is essential that the organization fully documents all elements of the BCMS and business continuity procedures and that these documents are maintained, controlled and stored appropriately. This is particularly important for any subsequent audits required for compliance assessment or certification against ISO 22301.

Clause 8: Operation

Clause 8.1, Operational planning and control, is a new clause and relates back to Clause 6.1, which requires the organization to identify the risks to the BCMS not being established, implemented and maintained by the organization. Clause 8.1 requires the organization to ensure processes that have been developed to manage the risks to the BCMS are being correctly implemented. This includes any processes that have been contracted-out or outsourced.

Clause 8.2.2, Business impact analysis, introduces a new term, 'prioritized timeframes'; however this is not listed in Clause 3, Terms and definitions. 'Prioritized timeframes' relates to the more familiar term, 'recovery time objective (RTO)', and defines the order and timing of recovery for critical activities that support the key products and services.

Although the term 'maximum tolerable period of disruption (MTPD)' is defined in Clause 3 it is not used in the body of the standard. However, Clause 8.2.2 c) does state that the organization must set prioritized timeframes for resuming activities that support the provision of (key) products and services 'at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable'.

Clause 8.2.3, Risk assessment, draws attention to the fact that 'certain financial or governmental obligations require the communication', at varying levels of detail, of the risks that could disrupt the prioritized activities. It goes on to advise that 'certain societal needs can also warrant sharing of this information', as appropriate.

Clause 8.4, Establish and implement business continuity procedures, brings together everything needed to deliver effective BCM procedures. The procedures must establish internal and external communications protocols, set out the immediate steps to be taken at the time of disruption but also be flexible to respond to changing circumstances and unanticipated threats. The BCM procedures must focus on impacts that could disrupt key products and services and be effective in minimizing the consequences of the disruption. This clause introduces the need to take account of stated assumptions and the organization's interdependencies.

Clause 8.4.2, Incident response structure, has expanded requirements, namely the need to 'identify impact thresholds that justify initiation of formal response' and the need, using life safety as the first priority, to implement external warnings and communications as appropriate. This is covered in Clause 8.4.3, Warning and communication, which is an entirely new requirement.

Clause 8.4.4, Business continuity plans, has fewer requirements than BS 25999-2. It does not require a named person to be designated as owner of the plan and be responsible for its review, update and approval. It does not require meeting locations and contact details to be included. It makes no specific reference to the need to include incident logs for recording decisions made and actions taken.

Clause 8.4.5, Recovery, is an entirely new requirement. The standard simply states that 'The organization shall have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident'. The looseness of this clause may lead to different interpretations across certification bodies.

Clause 8.5, Exercising and testing. ISO 22301 does not require an approved exercise programme to be in place. It does require the exercises to be based on an appropriate range of scenarios. It also links the review of the exercise back to the requirement to promote continuing improvement of the BCMS.

Clause 9: Performance evaluation

This clause brings together the maintaining and reviewing of the BCMS.

Clause 9.1, Monitoring, measurement, analysis and evaluation. This is a new set of requirements and is designed to ensure that appropriate metrics are in place to effectively manage the BCMS and provides the input to management reviews.

Clause 9.2, Internal audit. This clause now includes a requirement that the management responsible for the area being audited must 'ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.' Clause 9.2 drops the reference to taking into account the output of the BIA when developing an audit programme.

Clause 9.3, Management review. This is a very comprehensive clause. There is a new requirement to provide information for the review on the trends in

1. nonconformities and corrective actions
2. monitoring and measurement evaluation results
3. auditing results

Additionally, when considering the output from the management review changes may be required to risk reduction and security arrangements and operational conditions and processes, if appropriate. It may also be appropriate to change the measures for 'how the effectiveness of controls are measured'.

This clause concludes with a requirement for the organization to 'communicate the results of [the] management review to relevant interested parties, and take appropriate action relating to those results'.

The management review no longer has to take input from interested parties or consider the results of training and awareness programmes.

Clause 10: Improvement

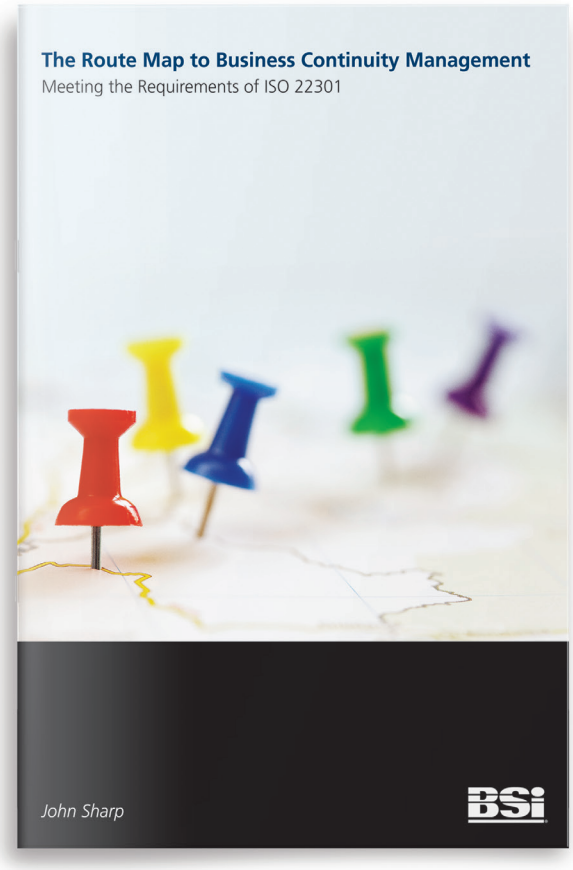
This clause combines the previous corrective and preventative actions under one heading: Nonconformity and corrective action.

Cross-references between BS 25999-2:2007 and ISO 22301:2012

BS 25999-2:2007	ISO 22301:2012	
	Directly related	**Does not cross reference**
Introduction	0.1 General 0.2 The Plan-Do-Check-Act (PDCA) model	
1 Scope	1 Scope	
2 Terms and definitions	3 Terms and definitions, some terms omitted, new terms added, some redefined.	
3.1 Planning the business continuity management system		4.1 Understanding of the organization and its context 6.1 Actions to address risks and opportunities (to the BCMS)
3.2.1 Scope and objectives of the BCMS	4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the management system 6.2 Business continuity objectives and plans to achieve them	

Cross-references between BS 25999-2:2007 and ISO 22301:2012

BS 25999-2:2007	ISO 22301:2012	
	Directly related	**Does not cross reference**
3.2.2 BCM policy	5.1 General 5.2 Management commitment 5.3 Policy	
3.2.3 Provision of resources	7.1 Resources 5.2 Management commitment 5.4 Organizational roles, responsibilities and authorities 8.3.2 Establishing resource requirements	
3.2.4 Competency of BCM personnel	7.2 Competence	
3.3 Embedding BCM in the organization's culture	7.3 Awareness 7.4 Communication	
3.4 BCMS documentation and records	7.5 Documented Information 8.1 c) Operational planning and control	
4.1.1 Business impact analysis	8.2.1 General 8.2.2 Business impact analysis	
4.1.2 Risk assessment	8.2.1 General 8.2.3 Risk assessment	
4.1.3 Determining choices	8.3.3 Protection and mitigation	
4.2 Determining business continuity strategy	8.3.1 Determination and selection 8.3.2 Establishing resource requirements	
4.3.2 Incident response structure	8.4.2 Incident response structure	8.4.3 Warning and communication
4.3.3 Business continuity plans and incident management plans	8.4.4 Business continuity plans	8.4.5 Recovery
4.4.2 BCM exercising	8.5 Exercising and testing	
4.4.3 Maintaining and reviewing BCM arrangements	9.1.2 Evaluation of continuity procedures	9.1 Monitoring, measurement, analysis and evaluation
5.1 Internal audit	9.2 Internal audit	
5.2 Management review of the BCMS	9.3 Management review	
6.1 Preventive and corrective actions	10.1 Nonconformity and corrective action 9.1.1 General	
6.2 Continual improvement	10.2 Continual improvement	



The Route Map to Business Continuity Management

Meeting the Requirements of ISO 22301

There are many factors that can create disruption to your business and cause failure to deliver services as normal or in extreme cases, failure to deliver at all.

By adopting a systems approach to BCM, organizations are better equipped to meet the challenges faced when a disruption occurs. Built around the requirements of BS ISO 22301, this book provides a practical approach to establish, implement, operate, monitor, review, maintain and improve an effective system for business continuity.

So whether you are planning to certify against the new standard or simply want to benefit from BCM best practice, this book delivers all the insight needed to get you off to a flying start.

You will be able to:

- Identify crucial risk factors already affecting your organization
- Understand your organization's needs and obligations
- Establish, implement and maintain your BCMS
- Receive a step-by-step guide on making the transition to the new international standard for BCM
- Gain confidence in your organization's ability to manage any disruption effectively

For more information, please visit: shop.bsigroup.com/bip2142

More Business Continuity Insight from BSI

Business Continuity Management for Small and Medium Sized Enterprises – How to Survive a Major Disaster or Failure by David Lacey

Don't think you have the resource to implement a business continuity system, or can't see the business justification? Then this is the book to get you started. Simple tried and tested approaches are set out to help businesses of any size keep customers happy during and after disruption – with minimum time and resources.

To download a free chapter, please visit:
shop.bsigroup.com/bip2217

A Practical Approach to Business Impact Analysis – Understanding the Organization through Business Continuity Management by Ian Charters

An effective business impact analysis (BIA) is vital to the success of any continuity plan. But what is it, and how do you do it? This book clearly explains the concept and benefits, as well as delivering a simple and practical method for conducting a BIA that meets the particular needs of your business.

To download a free chapter, please visit:
shop.bsigroup.com/bip2214

Auditing Business Continuity Management Plans – Assess and Improve Your Performance Against ISO 22301 by John Silltow

Why audit your BCM plans? One reason is that ISO 22301 requires an internal audit of the business continuity management system to be carried out by all organizations. Another is that it provides independent assurance that the system is adequate and properly managed. This book delivers in-depth information and knowledge needed by auditors to advise effectively on each part of the business continuity process.

To download a free chapter, please visit:
shop.bsigroup.com/bip2151

Business Continuity Communications – Successful Incident Communication Planning with ISO 22301 by Jim Preen

More than ever before, communication is a major factor in your organization's ability to emerge strongly on the other side of disruption. The bad news is that it is easy to get it wrong. The good news is that preparation is everything. Packed with practical examples, tips, checklists and templates, this book provides all you need to feel confident when communicating in a crisis, whoever your audience may be.

To download a free chapter, please visit:
shop.bsigroup.com/bip2185

Business Continuity Exercises and Tests – Delivering Successful Exercise Programmes with ISO 22301 edited by Jim Preen

How can you make sure that your business continuity plans will actually work if called in to action? By testing them. This practical book will help you decide which exercises and tests are appropriate to your business, according to likely risks. It also provides thorough, step-by-step guidance on carrying them out effectively. Case studies and scenarios make running your own exercises easier, as well as templates for recording and evaluating performance.

To download a free chapter, please visit:
shop.bsigroup.com/bip2143

John Sharp's biography

John Sharp FBCI (Hons), FCMI, MCIM is recognized worldwide for the contributions he has made to business continuity management. In 2004 he was made an Honorary Fellow of the Business Continuity Institute and at the 2004 BCM Awards in London was given a special award for his outstanding contribution to the industry. As a consultant, he has provided BCM advice to central and local government, the police, NHS and major international companies. He was chair of the committee that produced BSI's Guide to Business Continuity Management (PAS 56) and is a member of the Technical Committee that produced the BSI standard for BCM (BS 25999) and provided the UK contribution to the two Business Continuity International Standards (ISO 22301 & ISO 22313).

BSI
389 Chiswick High Road
London, W4 4AL
United Kingdom

T: +44 20 8996 9001
E: cservices@bsigroup.com
bsigroup.com