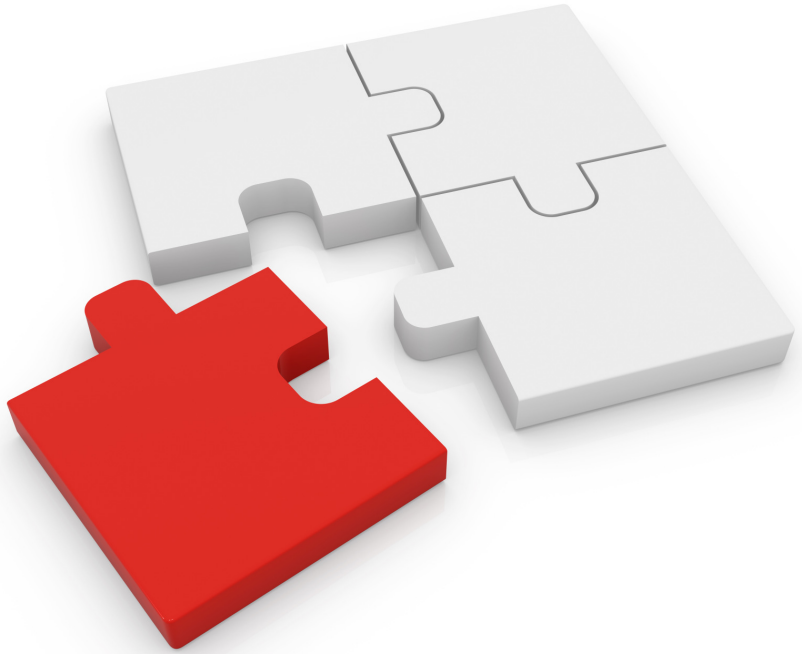
...making excellence a habit.™

# ISO 22301: Overview, certification and what to expect from your audit

Suzanne Fribbins, EMEA Product Marketing Manager - Risk

# Outline

- Overview of ISO 22301
- ISO 22301 – an implementation checklist
- The certification process
- Benefits of ISO 22301 certification
- Transitioning from BS 25999-2 to ISO 22301
- Potential areas of auditor focus



# Introducing ISO 22301

- ISO 22301 Societal Security - Business continuity management system - Requirements.
- Management system standard
- Based on global BCM consensus
- All core business continuity elements in BS 25999-2 are present in ISO 22301

# Societal Security and BCM?

- ISO 22301 now comes under a wider societal security remit
- This acknowledges the important role that BCM has to play in protecting society and ensuring our ability to respond to incidents, emergencies and disasters.

# Benefits of adopting a systems approach to managing BCM

- Allows organizations to benefit from global BCM best practice, regardless of whether they are planning to certify or not
- Provides a foundation and a common vocabulary for BCM best practice and guidance
- Consensus standards like ISO 22301 represent the input and recommendations of hundreds of BC professionals and industry experts
- Saves you having to reinvent the wheel

# Comparing ISO 22301 and BS 25999-2

Includes all core requirements

- The 'Plan Do Check Act' cycle
- Business continuity policy
- Business impact analysis
- Risk assessment and risk treatments
- Exercising
- Business continuity plans and strategy
- Internal audit
- Management review
- Non conformity and corrective action
- Improvement actions

# Key changes and aspects

Notable shifts in emphasis from BS 25999-2:2007:

- First standard written in accordance with Guide 83
- Change in the way an organization is defined
- Clearer expectations on management
- Preventive action has been replaced with “actions to address risks and opportunities” and features earlier
- ISO 22301 puts a much greater emphasis on setting the objectives, monitoring performance and metrics – aligning BC to top management strategic thinking

# Key changes and aspects

- 22301 requires more careful planning for and preparing the resources needed for ensuring business continuity
- Communication elements more demanding and there is a responsibility to the wider community defined
- BIA similar but with some changes to terminology
- There is a stronger link to the organizations approach to risk
- To reflect the societal security approach some new terminology has been introduced, see ISO 22300

bsi.

# New high level structure

- ISO 22301 is the first management system standard to be developed using Guide 83
- Guide 83 is for standards writers and provides a standardised text suitable for all ISO management system standards
- The intention is to standardise terminology and requirements for fundamental Management System requirements

# Structure of ISO 22301:2012

| Clause | Description |
|---|---|
| 4.0 | Is a component of Plan. It introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements, and scope. |
| 5.0 | Is a component of Plan. It summarises the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement. |
| 6.0 | Is a component of Plan. It describes requirements as it 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 business impact analysis (BIA) derived<br>recovery objectives. |

# Structure of ISO 22301:2012

| Clause | Description |
|---|---|
| 7.0 | Is a component of Plan. It supports BCMS operations as they relate to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documentation. |
| 8.0 | Is a component of Do. It defines BC requirements, determines how to address them and develops the procedures to manage a disruptive incident. |
| 9.0 | Is a component of Check. It summarises requirements necessary to measure BCM performance, BCMS compliance with the International Standard and management's expectations, and seeks feedback from management regarding expectations. |
| 10.0 | Is a component of Act. It identifies and acts on BCMS non-conformance through corrective action. |

# Clause 4: Context of the organization

- Clause 4 relates to the context of the organization which requires the organization to determine their external and internal issues
- There is now a clear requirement to consider interested parties
- This will determine its business continuity policy and objectives and how it will consider risk and the effect of risk on its business
- Requirement also for a procedure to manage legal and regulatory requirements

# Concept of interested parties

- ISO 22301 replaces the term ‘stakeholders’ with that of ‘interested parties’
- The ISO requires broader consideration of interested parties than BS 25999-2
- Closer alignment with organizational objectives for corporate social responsibility

# Clause 5: Leadership

- Clause 5 of the standard summarizes the requirements specific to top management's role in the BCMS
- Top management given clearer BCM responsibilities
- The ISO outlines specific ways in which management must demonstrate its commitment to the system

# Clause 6: Planning

- New section relating to establishment of strategic objectives and guiding principles for the BCMS as a whole
- When planning the BCM the context of the organization should be taken into account through the consideration of the risks and opportunities
- The organizations business continuity objectives must be clearly defined with plans in place to achieve them

# Clause 7: Support

- Clause 7 details the support required to establish, implement and maintain an effective BCMS, including:
  - Resource requirements
  - Competence of people involved
  - Awareness of and communication with interested parties
  - Requirements for document management.

# Clause 8: Operation

- ISO 22301 requires that organizations plan and control the operation of their BCM requirements. Most importantly this will include:
  - A methodology and documented process for conducting a business impact analysis (BIA)
  - A systematic methodology and documented process for conducting risk assessments
  - A methodology for selecting business continuity strategies which will protect the most important activities of the business and ensure their resumption in the event of disruption.


bsi.

# Clause 8: Operation

- ISO 22301 places greater emphasis on the procedure required to detect an incident, early communication thereof and the need to regularly monitor the incident
- There is also a requirement to consider how the organization will recover its activities from a temporary state back to "normal" (if appropriate)
- Exercises and tests to demonstrate the effectiveness of BCM arrangements

## Clause 9: Performance evaluation

- As with all management system standards there is a need to look back at what has been achieved
- ISO 22301 also requires that this analysis is evaluated and conclusions drawn by the organization
- Greater emphasis on setting of objectives, monitoring performance and metrics
- Most organizations will already produce metrics which can be tailored to BCMS performance

# Clause 9: Performance evaluation

- Internal audits and management review continue to be key methods of reviewing the performance of the BCMS and tools for its continual improvement

# Clause 10: Improvement

- Nonconformities of the BCMS have to be dealt with together with corrective actions to ensure they don't happen again
- As with all management system standards, continual improvement is a core requirement of the standard

# ISO 22301 - an implementation checklist

# ISO 22301 – an implementation checklist

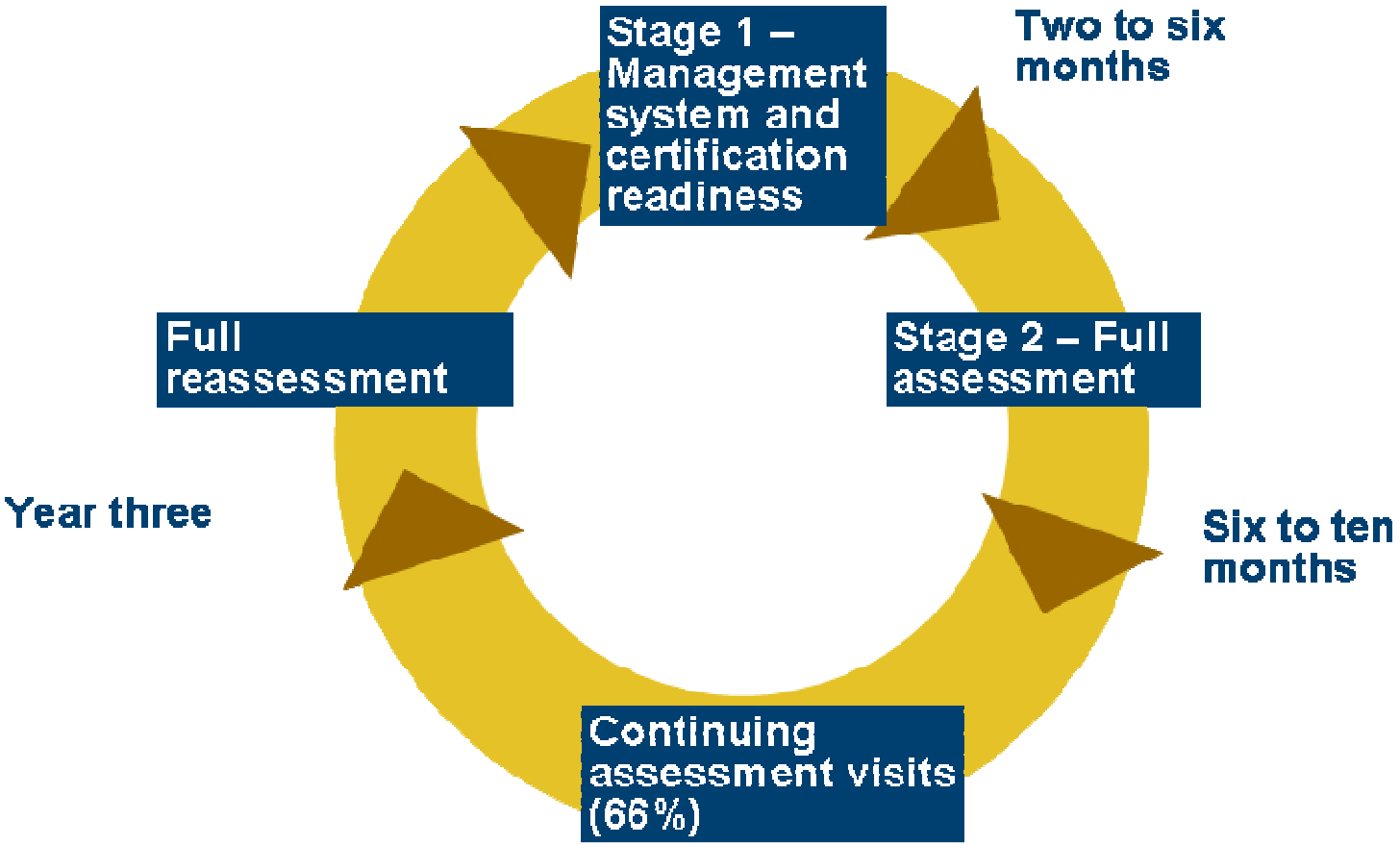
1. Obtain management support
2. Treat it as a project
3. BCM policy – define objectives and scope
4. Define roles and responsibilities
5. Implement mandatory procedures
6. Perform BIA and risk assessment
7. Determine the business continuity strategy

# ISO 22301 – an implementation checklist

8. Develop incident management plans and business continuity plans
9. Training and awareness
10. Exercising
11. Maintaining and reviewing the BCMS
12. Internal audit
13. Management review
14. Preventative and corrective actions

# Certification to ISO 22301 with BSI

# The assessment cycle for ISO 22301



# Benefits of certification

- Certification offers many advantages, including:
- It challenges your BCM programme and organization to reach a higher level of maturity and preparedness
- Supply chain requirement
- Prequalification for tenders
- Provides a competitive advantage
- Signifies a base level of readiness and a commitment and seriousness about BCM

# Transition period

**May 2012** — **November 2012** — **1 June 2014**

## Certification: BS 25999-2 or ISO 22301

**Organizations can choose to certify against either BS 25999-2 or ISO 22301**

## Certification: to ISO 22301

**After November 2012, BSI will only be offering certification to ISO 22301 to ensure that BS 25999 certified clients have an adequate amount of time to complete their transition**

## 2 year transition period

**Organizations will need to complete their transition to the new revision by 1 June 2014. Failure to do so will result in the expiry of their certificate.**

bsi.

How will the transition take place for existing customers?

- Assessment to the new standard will take place during continuing assessment visits
- A date for their transition will be agreed with their Client Manager
- A new certificate will be issued once they have demonstrated compliance with ISO 22301
- Clients can transition ahead of their next CAV for an additional fee

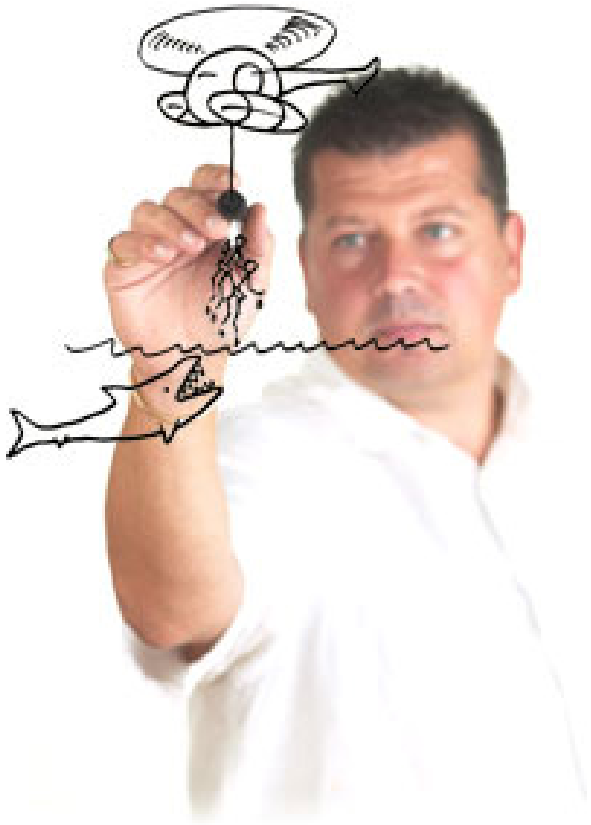
# Potential areas of auditor focus

# Potential areas of auditor focus

1. Exercising of business continuity procedures
2. Poor scoping – key resources/activities not included
3. BIA only considers inability to deliver products and services, not stakeholders or reputational damage
4. Lack of senior management commitment and culture of 'continual improvement'
5. Planned requirement to restore to BAU – does not cover all activities

# Exercising of business continuity procedures

- Business Continuity plans are useless unless you test them
- All elements of business continuity plans should be exercised on a regular basis
- Staff, vendors and stakeholders should be involved in exercises
- Keep exercises simple and realistic
- Team members need to be treated well
- Reports should be prepared post-exercise, and reviewed



bsi.

# Poor scoping - key resources/activities missing

# Business Impact Analysis is not comprehensive enough

- BIA needs to be comprehensive enough to meet the organization's needs while being simple enough for everyone to use
- It should not only consider the organizations inability to provide products and/or services and meet contractual agreements, but also damage to reputation and other stakeholder impacts, such as:
  - breaches of statutory duties or regulatory requirements
  - financial viability
  - deterioration of product or service quality
  - environmental damage

# Lack of senior management commitment

## Planned requirements to restore to BAU – does not cover all activities

- Section 8.4.5 requires 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.
- It is important that all prioritized activities are covered

# Next steps?

- Buy a copy of the new ISO 22301:2012
- Consider how the changes affect your organization
- Existing customers should speak with their Client Manager to agree timing for assessment to the new standard
- New customers can call BSI and speak with an advisor on +44(0) 845 080 9000 or visit www.bsigroup.co.uk/ISO22301

# How can BSI help you?

- Consider scheduling a BSI gap analysis
- Attend one of our new suite of training courses designed to help your organization with the new revision
  - The range includes introduction, transition, implementation and auditor courses
  - For more information, call the BSI training team on 0845 086 9000 or visit our website


bsi.

## Additional guidance available

- **Webinar – Transitioning from BS 25999-2 to ISO 22301** (available for download at https://bsiedge.bsi-global.com/iso22301transitionplan/)
- **Webinar – Introducing ISO 22301** (available for download at https://bsiedge.bsi-global.com/introducingiso22301-detailed/)
- **Transition guide** (available for download at http://shop.bsigroup.com/upload/Shop/22301-Transition-Guide.pdf). This free guide has been designed to help you meet the requirements of the new international standard for business continuity management, ISO 22301.
- Standards, books, BCM Self-assessment Tool, public and in-house training

bsi.

# Questions?

# Contact us

| | |
|---|---|
| Address: | BSI |
| | 389 Chiswick High Road |
| | London W4 4AL |
| Telephone: | +44 (0)20 8996 9001 |
| Email: | cservices@bsigroup.com |
| Links: | www.bsigroup.com |