Il nuovo standard ISO 22301 sulla Business Continuity
Scenari ed opportunità

Massimo Cacciotti — Business Services Manager BSI Group Italia
BSI: Introduction

1. Why we need BCM?
2. Benefits of BCM
3. International Development of BCM
4. Getting started with BCM
5. Related standard to BCM: ISO/IEC 27000 series
BSI’s Introduction

- Founded in 1901
- Global independent business services organization
- No owners/shareholders...all profit reinvested into business
- Standards, Assessment, testing, certification, training, software
- World’s #1 Standards Body
- #1 certification body in the UK, USA and Korea
- >2,500 staff and >50% non-UK
- 53 offices located around the world
- 70,000 clients in 150 countries
- £235m revenue in 2010

...making excellence a habit.
BSI’s Introduction

What our customers say about us...

- We have excellent people
- They would recommend us more than most
- 91% Is the average satisfaction rating of BSI client managers
- 80% of customers choose BSI because of its reputation
- They buy BSI on reputation and quality
- Our products deliver tangible, measurable benefits
- 80% of customers see benefits in ‘One BSI’
Our services

- Assurance Services (Assessment and Certification)
- Training
- Governance, Risk and Compliance
- Testing services
- Healthcare Services
- Advisory Services
We offer various types of training including:
- Awareness Training
- Implementation Training
- Auditor Training

Our delivery options:
- Public training courses
- In-house training course
- e-learning courses

Convenzione AIEA – BSI
BSI Governance, Risk & Compliance (GRC)

Entropy™ Software

- A turn-key solution that provides the management framework for fully functional integrated and auditable management systems including:
  - Environmental Management – ISO 14001
  - Health & Safety Management – OHSAS 18001
  - Quality Management – ISO 9001
  - Information Security Management – ISO/IEC 27001
  - Supplier Compliance Management (C-TPAT & AEO)
  - and other management systems standards
Business Continuity Management (BCM) facts and future trends
1. Why we need BCM

Definition

“Business Continuity Management (BCM) is a framework for identifying potential threats to an organization and building organizational capability to respond to such threats, in order to safeguard the interests of key stakeholders, reputation, brand and value-adding activities” (1)

(1) Joint statement: British Standards Institution, Business Continuity Institute, Cabinet office, Chartered Management Institute
Examples of Disruption

- Natural disasters
- Economic disruption and market turbolence
- Terrorism
- Physical security disruptions
- Infrastructure or IT failures
- Fraud or hacking
- New regulations

**Potential consequences:**
- Employee safety jeopardized
- Reduced customer confidence
- Loss in image or brand equity
- Decline in revenues
- Decline in market share
Are you prepared for disaster?
CMI/BSI UK survey – March 2011

- 84% of managers realize the benefits of BCM planning
- 58% of managers report that their organization has BCM in place (significant YoY growth in SMB sector)
- Only 50% of organizations with BCM test their BC plan once a year or more
- 60% of organizations with BCM provide training to relevant staff
- Only 55% of organizations ensure that their supply chain have BCM plans in place
2. BCM: The Benefits & Business Case

- Expedite recovery after disruption
- Understand overall business exposure
- Prepared to respond should the unexpected occur.
- Raises awareness in the organization
- Proxy for good overall management.
- Demonstrates to customers, partners and other stakeholders that the organization takes a robust approach to risk
- Reassurance that the business can keep going
Perceived benefits of BCM

- Improving business resilience: 79%
- Improve understanding of risk to organisation: 71%
- Reputation protection: 66%
- Meeting customer requirements: 61%
- Fulfilling statutory/regulatory requirements: 60%
- Competitive advantage: 34%
3. International development of BCM 25999

PAS 2003
• Started as a “PAS” (Publicly Available Specification) by BSI (PAS 56)

BS 2006
• Moved to a BS 25999 in 2006 & 2007 in two parts as “Umbrella Standard”

ISO 2012
• Scheduled to move to ISO in 2012 (ISO 22301)
International usage of BS25999

BSI

• BSI translations into French, German and Spanish
• BS 25999 sold by BSI in over 100 countries

Other National Standards Bodies

• Adoption of BS 25999 outside the UK (Brazil, Spain etc.)
• Local translation/distribution (Japan, China, Russia, etc.)

US

• As part of the ‘PS-Prep program’ the US Department for Homeland Security recommended 3 standards for BCM, including BS 25999.
The new ISO 22301

- The growing success of the BSI developed BS 25999 has prompted ISO (the International Organisation for Standardization) to begin work on publishing an ISO recognised standard which is expected to be released in **May 2012**

- BSI is well placed to assist clients in making a smooth transition to the new ISO standard in 2012 **(ISO 22301)**
4. Getting Started with BCM

Recommendations

- Senior managers must take ultimate responsibility for the quality and robustness of their organizations BCM.
- Use BCM based on a common framework (such as BS 25999) as part of a wider programme and train employees.
- Develop a clearly defined approach for responding to the media; BCM is “multi-functional” not just IT.
- Review which suppliers are critical to your operations and ask whether they have BCM.
- Test your BCM through regular exercises.
Introducing ISO 22301

• New international standard for business continuity management (BCM)
• Its official title is ISO 22301 Societal Security
  Business continuity management system - Requirements
• All core business continuity elements in BS 25999-2 are present in ISO 22301
What is ISO 22301?

• Provides the requirements for a business continuity management system (BCMS)
• Based on global BCM best practice
• Created in response to strong interest in the original British Standard BS 25999-2 and other regional standards
• BS 25999-2 key source text in its development
• For those certified to or aligned with BS 25999-2, the additional requirements are not onerous
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.
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 (leadership)
- 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 organization’s approach to risk
- To reflect the societal security approach some new terminology has been introduced, see ISO 22300
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
New concepts and activities

- Context of the organization
- Interested parties (now stakeholders)
- Leadership
- Maximum acceptable outage (MAO)
- Minimum business continuity objective (MBCO)
- Performance evaluation
- Prioritized timeframes
- Warning and communication
Plan – Do – Check – Act (PDCA) Cycle

Continual improvement of the Business Continuity Management System

Interested Parties

Plan
Establish

Act
Maintain and improve

Check
Monitor and review

Do
Implement and operate

Interested Parties

Managed Business Continuity

Interested Parties

Business Continuity requirements and expectations

Copyright © 2012 BSI. All rights reserved.
PLAN: Understanding the Organization

- Identify critical activities
- Perform Business Impact Analysis (BIA)
- Evaluate threats to critical activities
- Determine continuity requirements
- Determine choices
Business Continuity Policy

• Requires top management commitment and approval
• Includes objectives of business continuity and scope of business continuity management system
• Must be communicated
• Must be reviewed
• Should be appropriate to the nature, scale, complexity, geography and criticality of business activities
• Should reflect culture, dependencies and operating environment
PLAN: Determine Business Continuity Strategy

• Strategies are arrangements to enable an organization to recover
• Define and document incident response structure
• Determine how to recover each critical activity
• Manage relationships
DO: Developing and Implementing a BCM Response

- Incident response structure and Crisis Management
- Incident management plan
- Business continuity plan
Sequence of Events of an Incident

Overall recovery objective: back-to-normal as quickly as possible

Timeline

Incident Response

Within minutes to hours:
- Staff and visitors accounted for
- Casualties dealt with
- Damage containment/limitation
- Damage assessment
- Invocation of BCP

Business continuity

Within minutes to days:
- Contact staff, customers, suppliers, etc.
- Recovery of critical business processes
- Rebuild lost work-in-progress

Recovery/resumption – back to normal

Within weeks to months:
- Damage repair/replacement
- Relocation to permanent place of work
- Recovery of costs from insurers

Copyright © 2012 BSI. All rights reserved.
CHECK: Exercising, Maintaining, and Reviewing BC Arrangements

- Exercise program
- Exercise arrangements
- Maintaining BC arrangements
- Reviewing BC arrangements
ACT: Embedding BCM in Organizational Culture

- Ensure BCM becomes part of the core values and effective management of the organization
- BCM education for all employees
- Evaluate the effectiveness of the BCM awareness delivery
SUMMARY

• Disruptions experienced by 8 out of 10 organizations - a real threat
• 8 out of 10 say benefits & business cases are strong for BCM
• Despite this, many organizations still unprepared for BCM
• BS 25999 is the leading global standard to help implement BCM
• BCM should be reviewed with suppliers
• Media coverage included in BCM strategy (reputational risk)
• Senior managers must take ultimate responsibility for BCM
• Many tools to assist your organisations in BCM
The Early Adopters of BCM

...making excellence a habit™

The ICT and Finance sector are the early adopters of Business Continuity Management Systems.
<table>
<thead>
<tr>
<th>ISO/IEC 27000 Series</th>
<th>Description</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27000</td>
<td>Overview and vocabulary</td>
<td>2009</td>
</tr>
<tr>
<td>ISO/IEC 27001</td>
<td>Information security management systems - Requirements</td>
<td>2005</td>
</tr>
<tr>
<td>ISO/IEC 27002</td>
<td>Code of practice for Information security management</td>
<td>2005</td>
</tr>
<tr>
<td>ISO/IEC 27003</td>
<td>ISMS implementation guidance</td>
<td>2010</td>
</tr>
<tr>
<td>ISO/IEC 27004</td>
<td>Information security management - Measurement</td>
<td>2009</td>
</tr>
<tr>
<td>ISO/IEC 27005</td>
<td>Information security risk management</td>
<td>2011</td>
</tr>
<tr>
<td>ISO/IEC 27006</td>
<td>Guidance to Certification Bodies</td>
<td>2007</td>
</tr>
<tr>
<td>ISO/IEC 27007</td>
<td>Guidelines for ISMS auditing</td>
<td>2011</td>
</tr>
<tr>
<td>ISO/IEC 27008</td>
<td>Guidelines for auditors on information security controls</td>
<td>2011</td>
</tr>
<tr>
<td>ISO/IEC 27010</td>
<td>Guidance for inter-sector and inter-organizational communications</td>
<td>2012</td>
</tr>
<tr>
<td>ISO/IEC 27011</td>
<td>Guidance to telecommunications</td>
<td>2008</td>
</tr>
<tr>
<td>ISO/IEC 27031</td>
<td>Guidelines for ICT readiness for business continuity</td>
<td>2011</td>
</tr>
</tbody>
</table>
Other 27000 standards in development

ISO/IEC 27013  
Guidelines on the integrated implementation of ISO/IEC 27001 & ISO/IEC 20000-1  
(2012)

ISO/IEC 27014  
Governance of information security  
(2012)

ISO/IEC 27015  
Information security management guidelines for financial services  
(2013)

ISO/IEC 27016  
Information security management – Organizational economics  
(2014/15)

ISO/IEC 27017  
Information Security in Cloud Computing (relevant controls in 27001)  
(2014)

ISO/IEC 27018  
Information Security in Cloud Computing (relevant controls in 27001 - DP/Privacy)  
(2014)

ISO/IEC 27032  
Guidelines for cyber-security  
(2012)

ISO/IEC 27034  
Guidelines for application security (6 part standard)  
(2012…)

ISO/IEC 27036  
Information security for supplier relationships (4 part standard)  
(2012/13)

ISO/IEC 27037  
Guidelines for identification, collection, acquisition and preservation of digital evidence (possibly a 4 part standard)  
(2013/14)

ISO/IEC  27038  
Specification for digital redaction  
(2013)
bsi.

...making excellence a habit™