

An introduction to best practice standards for resilience

© The British Standards Institution 2011

Lorraine King – Product Marketing Manager BSI

THINGS AREN'T
AS BAD AS THEY SEEM
- I BACKED UP EVERYTHING
ONTO MY LAPTOP THAT'S
AT HOME!



Who is BSI?

- Founded in 1901
- Leading worldwide business services provider
- Clients in over 110 countries, over 2,300 employees



the development, sale and distribution of private, national and international standards

product testing services and Kitemarking

independent assessment, certification and training of management systems standards



What is a standard?

- An agreed, repeatable way of doing things
- A full consensus of all interested parties, so not imposed
- Voluntary
- *Best* practice not general practice, thus aspirational
- Compliance is measurable
- Kept current through regular updates



Business continuity management?



International Survey Results 2010 - PwC

- Within the worst economic downturn in 30 years, information security has an “enormously important” role to play. Tackling information risks associated with:
 - New Business Models, M&A transactions, Lay offs, changing regulatory landscape, cross organisation cost cutting, social networking
- Global leaders are protecting the information function from cuts but putting it under intense pressure to perform
- Protecting critical data elements in the organisation is a top priority at this critical time

Source - The global state of information security survey 2010 - PwC

In other news

- Cyber crime is now considered to be one of the biggest security threats facing the UK.
- UK Government National Security Strategy
 - Tier one threat
- Information and data security critical to many core UK industries

Standards and Resilience

- Business Resilience
 - Adaptability
 - Responsiveness
 - Opportunistic
 - Sustainability

Management systems

Competency

**Buy in and
ownership**

**Plan, do,
check, act**

**Continuous
improvement**

**Corrective
and
preventative
action**

Auditing

Third party certification

The issue of a certificate by an independent, external body, following audit and assessment against a defined set of requirements.

*An accredited certification can only be conducted by a certification body that is accredited with a recognised national body
e.g. UKAS*

BS 25999 – The standard for business continuity

© The British Standards Institution 2011

Lorraine King – Product Marketing Manager BSI

BS 25999 Contributors and Committee



In development the standard received more comments than any other published standard, including input from both public and private sector.

Standards and Guidance

BS 25999 – 1, The Code of Practice December 2006

BS 25999 – 2, Specification November 2007

ISO 27031, Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity March 2011

PD 25111, Human aspects of business continuity September 2010

PD 25666, Exercising and testing for continuity and contingency programmes July 2010

Main sections of the standard

- Overview of Business Continuity Management
- The Business Continuity Management Policy
- BCM Program Management
- Understanding the Organisation
- Determining BC Strategy
- Developing and Implementing a BCM Response
- Exercising, Maintenance and Review Arrangements
- Embedding Business Continuity Management into The Organisational Culture

“We know that mobile communications are an essential service for all businesses – retaining BS 25999 certification demonstrates that we continue to deliver a reliable and high quality network for our customers, no matter what.”

**Peter Kelly, Enterprise Director,
Vodafone UK**

“The rigour required to achieve certification has resulted in more comprehensive risk assessments, better staff training and awareness. It has also created opportunities for improvement, such as the acquisition of additional equipment assessed as being potentially life saving in the event of a loss of key resources.”

Lynne Watkins, Joint Divisional Head of Nursing, Emergency Department, Kings College Hospital

ISO/IEC 27001 – The standard for information security

© The British Standards Institution 2011

Lorraine King – Product Marketing Manager BSI

Standards and Guidance

ISO/IEC 27001, Specification October 2005

ISO/IEC 27002, The Code of Practice June 2005

ISO/IEC 27003, Implementation guidance February 2010

ISO/IEC 27004, Measurement January 2010

ISO/IEC 27005, Risk Management June 2008

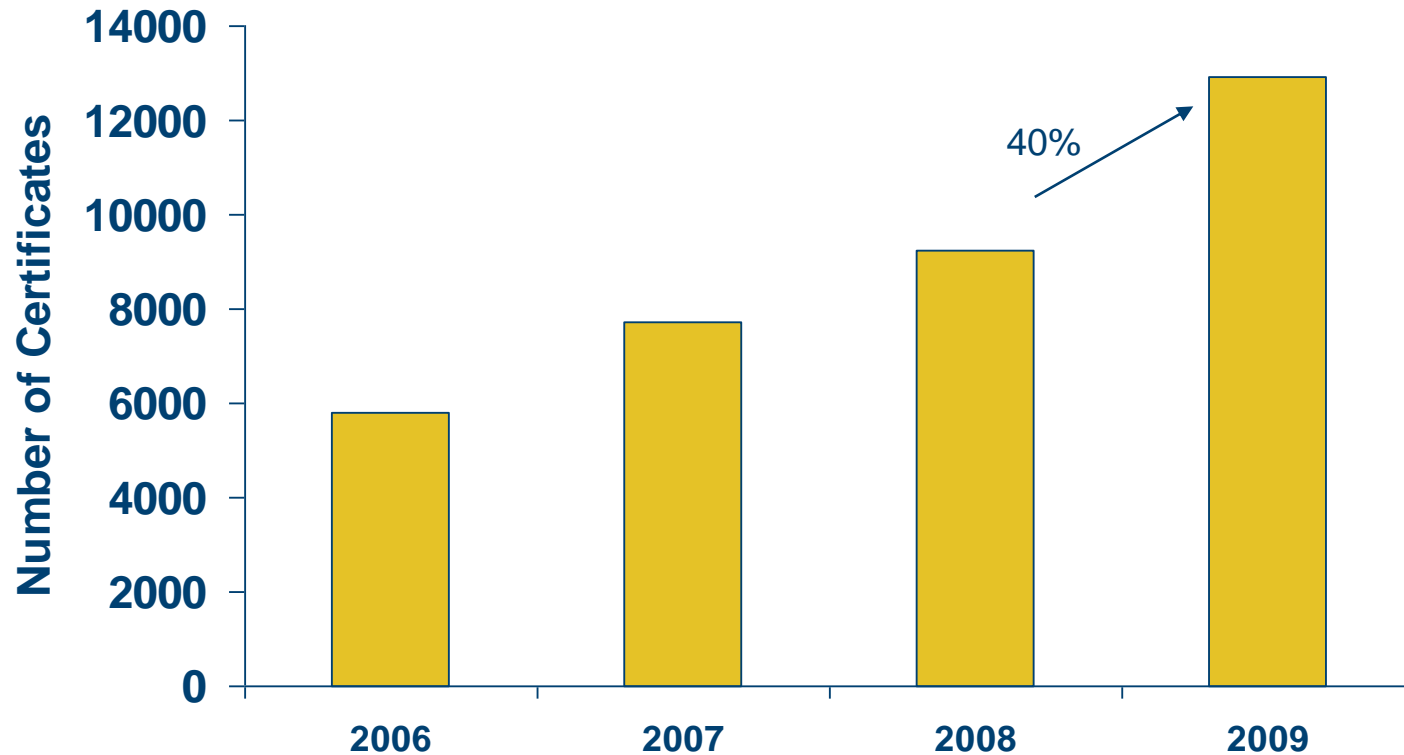
ISO/IEC 27000, Overview July 2009

1. Security Policy.
2. Internal Organization.
3. Asset Management.
4. Human Resources Security.
5. Physical and Environmental Security.
6. Communications and Operations Management.
7. Access Control.
8. Information Systems acquisition, development and maintenance.
9. Information Security Incident Management.
10. Business Continuity Management.
11. Compliance.

***11 sections,
each with specific
aims and focus:***

133 control statements

Global growth in certification



In a recent study*

- Over 80% of information security managers reported that ISO 27001 had delivered a positive impact to their organisation
- Key benefits included
 - Increase in ability to meet compliance requirements
 - Increase in customer satisfaction
 - Increase in competitive position
 - Decrease in security incidents and risk

**BSI sponsored research 2011*

“Although we have only recently gained certification to ISO 27001, there are at least three recent incidences where Cleardata has won contracts as a result of certification. The process ensures that we stop to think about all aspects of our security and continually monitor and improve, keeping us a step ahead of many of our competitors.”

David Bryce, Managing Director
– Cleardata

BCM does not neglect disaster recovery,
but it sees it as a sub category.

I DON'T CARE
IF YOU'RE THE MOTHER
OF ALL VIRUSES - I'VE
GOT OUR BCM PLAN
IN PLACE!



Thank you for your time

Lorraine.King@BSIGroup.com

© The British Standards Institution 2011