

Certification v Compliance – which should I focus on?

by John Hele , Global Product Manager, BSI Management Systems

Presentation content

- Business continuity
- Standards involved
- Definitions
- Compliance vs Certification
- Why Compliance *and* Certification
- Conclusions

Business Continuity

- The key word is 'continuity'!
- This is all about an organizations ability to 'continue' to provide products and services.
- How does an organization ensure it continues to provide those products and services?
By establishing their threats and risks and having controls in place to manage their systems.
- How do you ensure those controls are adequate?
By introducing management systems that will provide a framework for those controls.

Standards involved.....

- SS 540 Business Continuity Management (Singapore)
- BS 25999 Parts 1 and 2 Business Continuity Management (UK)
- BS 31100 Risk Management (UK)
- MS 1970:2007 ;
Business Continuity Management - Framework
- And other ISO standards – including ISO PAS 22399 on organizational continuity

What is Business Continuity Management?

business continuity management (BCM)

a holistic management process that identifies potential threats to an organization and the **impacts** to business operations that those threats, if realized, might cause, and which provides a framework for building organizational **resilience** with the capability for an effective response that safeguards the interests of its key **stakeholders**, reputation, brand and value-creating activities

*NOTE Business continuity management involves managing the recovery or continuation of business activities in the event of a business disruption, and management of the overall programme through training, **exercises** and reviews, to ensure the **business continuity plan** stays current and up-to-date.*

This is to demonstrate that it's a company wide implementation, is based on risk and provides a framework for building resilience and capability to protect the business.

Source: BS 25999-2

Definitions:

- **Compliance**
Action of a person or body in fulfilling the requirements of a law, standard or other rule
- **Certification**
Refers to the confirmation of certain characteristics of an object, person, or organization by another (preferably independent and authorized) body

Compliance

- What will you be compliant with?
 - Standards
 - Non prescriptive Management Systems that provide the framework for BCM - such as BS 25999, or
 - Specification type Management Systems which include prescriptive requirements as well as providing a framework - such as SS 540
 - Regulation
 - Prescriptive
 - Clients' requirements
 - Prescriptive
 - Internal requirements
 - Prescriptive
 - All of these? Management Systems standards can provide the framework to build the '*prescriptive requirements*' around

Certification

- What is certification given against:
 - Standards
 - BS 25999
 - SS 540
 - ISO standards, ISO 9001, ISO 27001 etc
 - Regulations
 - National regulations
 - Local regulations

Why Compliance?



Why Certification?



Conclusion - You need both!

- Compliance to show:
 - Commitment to meeting regulation
 - Commitment to meeting clients requirements
 - Commitment to stakeholders
- Certification to 'prove' compliance:
 - External verification of your commitment to stakeholders
 - Shows current and potential customers that you are in control
 - You are serious about the continuity of your organization
 - You are open to suggestions for improvement.

You can't predict the incident,
but you can predict the outcome.

The likelihood of something very unlikely
happening, is very likely!

If you think business continuity
is expensive, try having an incident!

“It’s not the strongest of the species that survives, nor the most intelligent, but the ones most responsive to change”

Charles Darwin

End of Presentation