

The use of Certification for Business Continuity

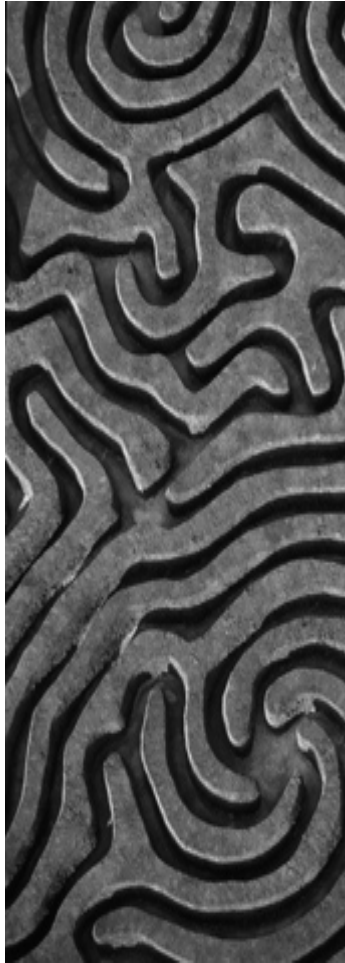
LSEC - Continuity Management Revisited

28 April, 2009

Harry Crosiers

 **ERNST & YOUNG**
Quality In Everything We Do

Agenda



- ▶ Introduction to Certification
- ▶ Why is Certification important ?
- ▶ Who can/should certify ?
- ▶ Certification based on what ?
- ▶ Certification of Business Continuity
- ▶ Certification programme for Business Continuity
- ▶ The Certificate
- ▶ Questions & Answers

Introduction to Certification

- ▶ Terminology

- ▶ Certification

- ▶ the confirmation of certain characteristics of an object, person, or organization; this confirmation is often, but not always, provided by some form of external review, education, or assessment (*Wikipedia*)
 - ▶ the successful conclusion of a procedure to evaluate whether or not a professional activity actually meets a set of requirements
 - ▶ ISO : procedure by which a third party gives written assurance that a product or service conforms to specified requirements

- ▶ Attestation

- ▶ Attest : To affirm to be correct, true, or genuine
To certify by signature or oath

Introduction to Certification

- ▶ Terminology (cont'd)
 - ▶ Accreditation
 - ▶ is a process in which certification of competency, authority, or credibility is presented
 - ▶ Procedure by which an authoritative body gives formal recognition that a body, or person, is competent to carry out specific tasks

Why is Certification important ?

- ▶ Highlights:
 - ▶ Stimulus for improvement
 - ▶ Following the certification principles helps
 - ▶ Certificates are meaningful for comparison with competitors
 - ▶ Loyalty instrument to attract customers

- ▶ The unjustified issuing of a certificate may damage the reputation of the whole scheme

- ▶ Requires a clear description what it stands for
- ▶ Certification (value) is very subjective and market-driven
- ▶ Value of certificate is only as high as its reputation

Who can/should certify ?

- ▶ The concept of “certifying organisation” is not protected
- ▶ In principle any private or public entity can issue certificates
- ▶ To obtain recognition by government, a certifying authority has to be “accredited”
 - ▶ Can install an accreditation mechanism guaranteeing the quality of certifying organisations
 - ▶ Can directly empower organisations to issue certificates
- ▶ Independence from interested parties is required

Certification based on what ?

- ▶ Certification schemes (frameworks)
 - ▶ ISO-standards
 - ▶ Common criteria
 - ▶ AICPA's Statements on Auditing Standards (SAS 70, WebTrust, SYSTrust, ...)
 - ▶ BSI's 25999 part 2 Business Continuity Management

- ▶ Choice of Certification scheme
 - ▶ Scheme that builds trust between parties
 - ▶ Provides useful information, rather than just a certificate
 - ▶ Certificate must be relevant for performed activities

Certification programme for Business Continuity

- ▶ BS 25999-2
 - ▶ Initial certification audit is conducted in 2 stages
 - ▶ Audit client's management system documentation
 - ▶ Evaluate implementation of the client's management system
- ▶ Relation with ISO/IEC 27001/2

- ▶ Everything that comes with a value has a price
 - ▶ Documentation
 - ▶ Procedures
 - ▶ Training
 - ▶ Testing ??

Certificate

- ▶ Expected to provide evidence of
 - ▶ Competence (people), or
 - ▶ Quality (product or process)
 - ▶ Actually shows only compliance !
 - ▶ Checking documentation vs Testing effectiveness
 - ▶ Certification should not be about what something is, but about how to use it
- ▶ Scope needs to be clearly stated as well as the value
 - ▶ Design and implementation of documentation, process vs operating effectiveness
 - ▶ Evaluation method(s): examination, test, checklist, ...
- ▶ Should be valid only for a limited time period (max. 1 year)

Certification over the next years

- ▶ A certificate does not guarantee success, but not having a certificate does not imply failure
- ▶ Certification against recognised standards will continue to gain wider acceptance
- ▶ Challenge to determine which standards
- ▶ Value of certificate is only as high as its reputation

Business Continuity

Step 1 - Understand the organization

Perform a business impact analysis (BIA) to identify processes and internal & external dependencies that are critical for your company's survival. Establish minimal guaranteed client service levels for critical processes. Conduct a risk assessment (RA) to identify potential continuity threats & risks and propose a risk action plan.

- ▶ Business impact analysis
- ▶ Risk assessment & action plan

Step 2 - Define the strategy

Develop a business continuity strategy based on the outcome of the first step. Present alternative recovery strategies for processes & critical assets (ICT, facilities, and personnel) for executive decision making. Define your company's internal & external business continuity policy.

- ▶ Business continuity strategy
- ▶ Internal & external business continuity policy

Business continuity planning

Define a customized exercise program, a maintenance- and an awareness campaign. Translate the exercise program into a test plan and scenarios. Organize, conduct and review tests for all aspects of the business continuity plan.

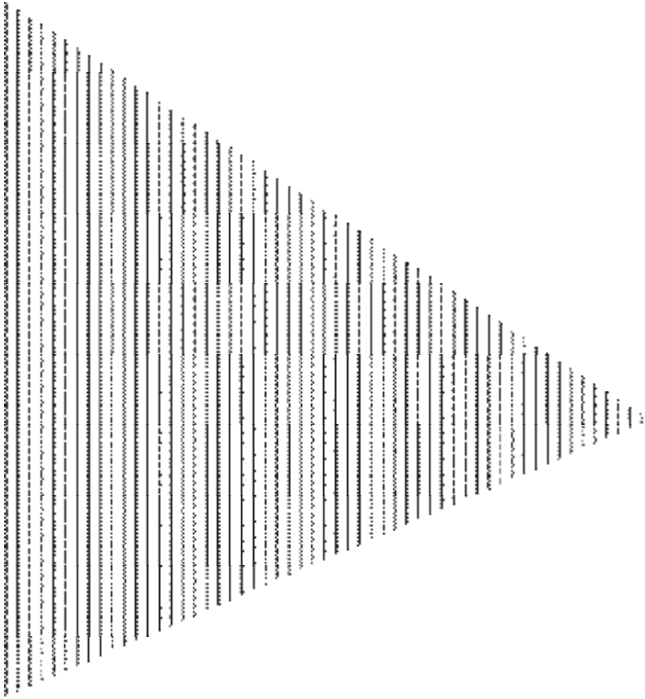
- ▶ Exercise program
- ▶ Maintenance and awareness campaign
- ▶ Test plan, scenario & review report

Step 4 - Test & maintain

Define and assign roles & responsibilities of the resilience organization with special attention to crisis management. Document the business continuity plan & procedures (BCP) for the critical business processes and supporting processes, including facilities and the ICT disaster recovery plan (ICT DRP).

- ▶ Business continuity roles & responsibilities
- ▶ Business continuity plan & procedures

Step 3 - Develop the BCP



Thank you

 **ERNST & YOUNG**
Quality In Everything We Do