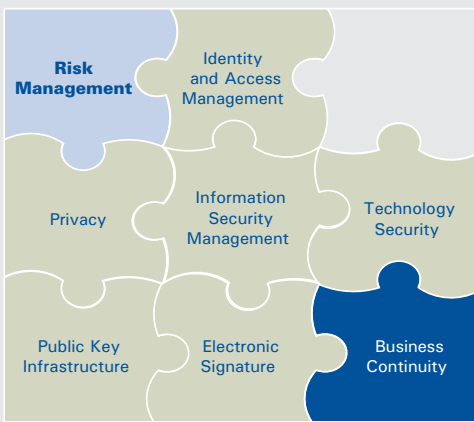


Business Continuity Management

ADVISORY



An organization's inability to react flexibly and swiftly when disaster strikes, and its inability to recover in a reasonable timeframe, may result in various consequences including loss of revenue, defection of customers, deterioration of brand equity and permanent loss of shareholder value. A KPMG study shows that 40 per cent of organizations who suffer a disaster go out of business within two years. And yet, information technology (IT) failures account for nearly 60% of all business interruptions as organizations become increasingly dependent on IT services.

Faced with rising exposure to new risks and a decreasing tolerance for disruptions to their operations, many organizations find it prudent to evaluate their ability to respond

to crises and mitigate possible future risks. These companies want to protect their employees and they understand that the ability to perform and satisfy customers is fundamental to sustaining competitive advantage. Environment becomes more complex:

- Organizations are becoming increasingly dependent on information technology (manual alternatives are no longer possible).
- The number of dependencies in the chain is increasing, and so is liability.
- The trend towards consolidation and concentration continues (within organizations: shared service centers).
- Traditional ICT controls (contingency backup and IT disaster recovery planning) do not meet high availability requirements.
- Organizations are dependent on external service providers (outsourcing, need to set up service level management).

KPMG addresses such issues through a three-level approach. The first level covers Disaster Recovery Planning (DRP) after an unforeseen event; the second level ensures continuity of business processes through Business Continuity Planning;

while the third level focuses on ensuring the seamless availability of critical information for business services. This vision is depicted in the diagram below. An increasing number of electronic and ICT device failures and their possible business impact raise the importance of bringing together business and IT decision makers.

Our approach

KPMG member firms, which make up part of a global network, have developed a proprietary Business Continuity Management (BCM) Methodology that is fully aligned with generally accepted standards in this and related areas, such as BS 25999, BSI PAS 56, ISO/IEC 17799, Cobit or ITIL.

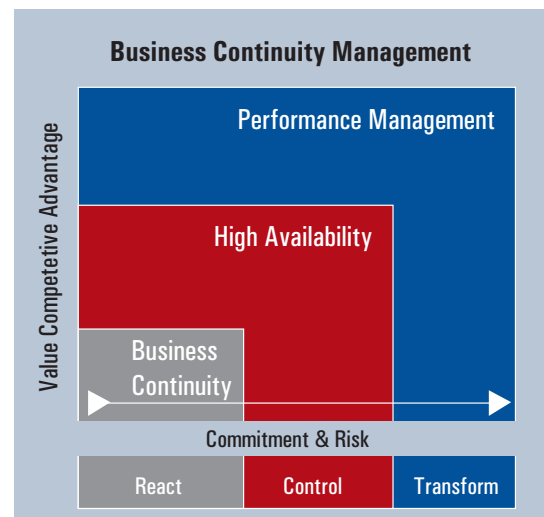


Diagram 1

Source: KPMG

The development of this methodology is coordinated by several KPMG Centers of Excellence which support local teams realizing BCM projects all over the world. The global methodology is then customized to the specific needs and environment of individual clients. The methodology identifies four BCM life-cycle stages depicted in the Diagram 2.

Benefits of implementing a BCM project with KPMG in Slovakia

Our clients benefit from the following:

- Utilizing our knowledge of business drivers and processes in several sectors and linking it to the client's BCM governance framework and implementation;
- Linking BCM into organization's operational risk management, regulatory frameworks (e.g. Basel II) and security and information governance;
- Identification of an effective recovery strategy consistent with business rather than purely ICT needs;
- Structured approach based on a flexible, modular methodology;
- Aggregated BCM skills and experience within a national network with access to resources of the global KPMG network;
- Project management and timely project completion where an organization's internal resources may not be available;
- Knowledge transfer as we work with client teams during development and delivery of project deliverables;
- A coordinated and scalable Business Continuity Planning strategy and Disaster Recovery (DR) solution;
- Proactive knowledge of the regulatory environment and constantly evolving BCM best practice.

Contacts



Peter Borák, CISA, CISM, CISSP
Partner, Advisory
Security, Privacy and Continuity
e-Mail: pborak@kpmg.sk



Pavol Adamec, CISA, CISM, CISSP
Director, Advisory
Security, Privacy and Continuity
e-Mail: padamec@kpmg.sk



Július Šiška, CISA, CISM
Manager, Advisory
Security, Privacy and Continuity
e-Mail: jsiska@kpmg.sk

KPMG Slovensko spol. s r. o.
Mostová 2
811 02 Bratislava
Tel.: +421 (0)2 59 98 41 11
Fax: +421 (0)2 59 98 49 99
www.kpmg.sk

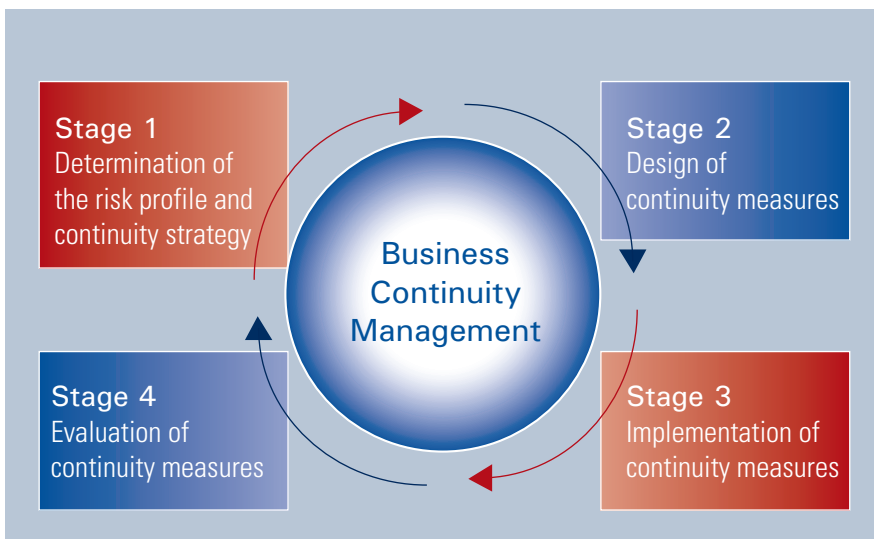


Diagram 2

Source: KPMG

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2008 KPMG Slovensko spol. s r.o. a Slovak limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative.
All rights reserved. Printed in Slovakia.

March 2008