Keys to Resilience for Small and Medium Enterprises
Agenda

- Risks to Resilience
- IBM Resilience Framework
- Resilience Lifecycle
- Conclusion
Today’s businesses need to reduce expenses and manage risk while maintaining continual availability to data and services.

**Mobile in the enterprise**

**90 percent** of organizations will support corporate applications on personal devices by 2014

**Innovation in the cloud**

**60 percent** of chief information officers view cloud computing as critical to their plans

**Increased outage costs**

38 percent

Increased to US$182 thousand per hour in two years from 2010-2012

**Budgetary constraints**

71 percent

of the average IT budget is dedicated to ongoing operations

**Unplanned IT outages**

70 percent

of organizations surveyed list this as their primary concern

**Exploding data growth**

40 zettabyte

of digital content in 2020, a 500 percent increase from 2010

**Aging infrastructure**

71 percent

of data centers are over 7 years old

---

External threats are increasing globally, with economic losses from all types of disasters escalating rapidly.

2012 natural catastrophes

Number of events: 905

- **Geophysical events** (earthquake, tsunami, volcanic activity)
- **Meteorological events** (storm)
- **Hydrological events** (floods, mass movement)
- **Climatological events** (extreme temperature, drought, wildfire)

Source: Münchener Rückversicherungs-Gesellschaft, Geo Risks Research, NatCatSERVICE, January 2013
The increasingly connected world has magnified the impact on every aspect of life, including its disruptions.

- 90 percent of the worldwide (WW) Bismaleimide-Triazine (BT) resin supply stopped\(^1\)
- World-wide car production was down by 20-30 percent for some major auto manufacturers during April and May\(^2\)
- The percentage of visitors to Japan dropped to 60 percent in April\(^3\)
- The Iceland volcanic eruption cost airlines US$1.7 billion with more than 10 million people affected\(^4\)
- Personal information leaks have cost millions of dollars, led to class action law suits, and damaged corporate reputation
- Hosting provider service outages affect Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) for other vendors

1Update: Analysts fear shortage of key resin, Dylan McGrath, 17 March 2011
2Japan's Earthquake and Tsunami Hit Parts Supplies, Motor Trend, June 2011
3Japan's tourism industry recovering after the tsunami, BBC Business News, 6 October 2011
4Volcano Crisis Cost Airlines $1.7 Billion in Revenue - IATA Urges Measures to Mitigate Impact, IATA Pressroom, 21 April 2010
IBM’s Resilience Framework depicts a comprehensive view of an Enterprise Resilience program.

To deliver a total resilience program, the resilience capability of each layer must be optimized.
True resilience requires a lifecycle methodology to achieve sustainable improvements.

**Business imperatives:**
- IT risk management
- Regulatory compliance
- Corporate governance
- Reputation

**Operational risk management**

**Inputs:**
Business objectives, goals, priorities, policies and current capabilities

**Outputs:**
Reduced risk, improved governance and facilitated compliance management

**Diagram:**
- **Plan:** Define, Design, Deploy, Validate
- **Implement:** Monitor, Control, Analyze, Evaluate
- **Manage:** Assess

© 2014 IBM Corporation
To build a business resilience program, you must first assess your potential risks, their impact and your ability to mitigate them.

Assess

- Analyze current and potential risks, and establish a risk profile by location, line-of-business function and business process.
- Determine impact of event: financial, opportunity and reputation.
- Evaluate mitigation capabilities to develop customized risk framework
- Identify areas for further analysis.
- Assess maturity of mitigation capabilities, including basic, managed, predictive, adaptive and resilient capabilities.

Diagnose risks to business objectives and prescribe appropriate actions to improve business resilience.
Enterprise-wide risks need to be identified, prioritized and addressed as you design and develop your business resilience programs.

**Plan**

- Set objectives for risk mitigation or enhancement to help:
  - Define the scope for the risk strategy.
  - Select the risks that need to be mitigated or enhanced

- Define strategic business continuity, disaster recovery and crisis management plans to help sustain critical operations in the event of a disruption

- Design for business resilience:
  - Business and financial justification
  - Governance and authority and policies
  - Systems management disciplines
  - Physical and logical security
  - Application and data
  - Program execution
  - Facilities

*Improve your business resilience with cost-optimized, IT resilience architectures, plans, procedures and strategies.*
Validate IT recovery plans, procedures, and processes meet business resilience requirements through appropriate testing.

**Implement**

- Choose resilient partners for your resilience solutions, including data storage and Disaster Recovery

- Deploy business resilience program:
  - Implement resilience architecture, processes, and organization structure
  - Document resilience programs and train key personnel

- Validate business resilience plans and procedures
  - Architect and execute tests of defined resilience plans to help confirm they meet specified objectives:
    - Protection of critical information
    - Recoverability of business functions
  - Execute tests or perform walkthrough drills to identify resilience plan weaknesses for improvement and preparedness

*Identify resilience plan issues and gaps to be addressed before a disruptive event occurs.*
A centralized governance program is critical for managing and maintaining a sustainable business resilience program.

Manage

- Monitor current conditions to detect and respond to risks.
- Control negative risk while enhancing positive risk.
- Maintain compliance with regulatory requirements
- Report on performance utilizing resilience dashboards to demonstrate readiness and results of business investment in resilience

Re-assess

- Perform periodic assessments to validate that resilience plans still address business strategies and risks
- Perform continuous improvement

Helps ensure a state of readiness to respond to an outage event or a market opportunity.
Conclusion

- Surviving in a competitive business environment requires continuous availability of IT systems and data, even in the event of a disaster.
- Businesses can face revenue loss and erosion of customer trust if they fail to maintain continuity while rapidly adapting and responding to risks and opportunities.
- You need to create, implement and manage a business resilience strategy that centers on identifying and mitigating prioritized risks across your enterprise.
- It is critical to choose resilient partners as you implement your enterprise resilience strategy.
- IBM’s recommended lifecycle methodology helps you achieve more sustainable improvements in business resilience, optimize cost and better manage risk and compliance.
Thank you for your time today.

For more information:

- IBM Resiliency Consulting Services
- IBM Business Continuity and Resiliency Services

Contact:

- IBM Taiwan BCRS Solution Sales Manager
  *Samuel Tsai*

  cytsai@tw.ibm.com
  Tel :886-2-87239666