

Implementing Business Continuity Management - a smart way

Nalin Wijetilleke
MBA,CISA,PMP,CBCP,MBCI
President – ISACA UAE Chapter

Abstract



- Among the top concerns of the CEOs and CIOs, Business Continuity is a priority. It has become a key necessity for survival in today's turbulent and technology based economy.
- Hence Business Continuity has to be ensured and implemented as a discipline and not merely as a audit requirement. This presentation throws some light, how best it can be achieved.

© Nalin Wijetilleke

Agenda



- Scope & Definitions
- Drivers of Business Continuity Management
- Risk Mitigation as the core purpose
- The SMART approach – step by step
- Strategy Development
- Crisis Management
- Exercising & Testing
- Summary

© Nalin Wijetilleke




Should organizations
have
Business Continuity
Management?

ISACA
Sri Lanka Chapter

Common reasons for Unpreparedness

- Denial
- Lack of awareness of the potential harm
- Inability to learn from others or own experiences

Anything which will prevent you achieving Business Objectives is a RISK



© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Common Terms

- Incident: An event if not controlled would lead to multiple impacts
- Disaster: A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability of an organizations part to provide critical business functions

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Common Terms

- Business Continuity Management
Holistic management process that identify potential impacts that threaten an organization and provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, brand and value creating activities.
BCM must be fully integrated into the organization as an embedded management process.
Ref. BCI Good practice Guidelines 2008

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Common Terms

- Business Continuity Plan
 - Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable the organization to continue to deliver critical activities at an acceptable predefined level
- Disaster Recovery Plan
 - Documented collection of procedures and information needed to resume normal computing capabilities associated with business critical processes
- Business Impact Analysis
 - Actions to identify customer impacts, financial impacts, reputational impacts and other related business impacts and raking them based on their criticality for business continuity

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Recent Disasters

- Earthquake in China
- Cyclone in Myanmar
- Huge FOREX trading loss at a French Bank – USD 7.14m
- Personal Data Loss of 37000 customers of UK Bank
- Asian Tsunami
- Pakistan: 100 die in Taliban suicide bombings

© Nalin Wijetilleke

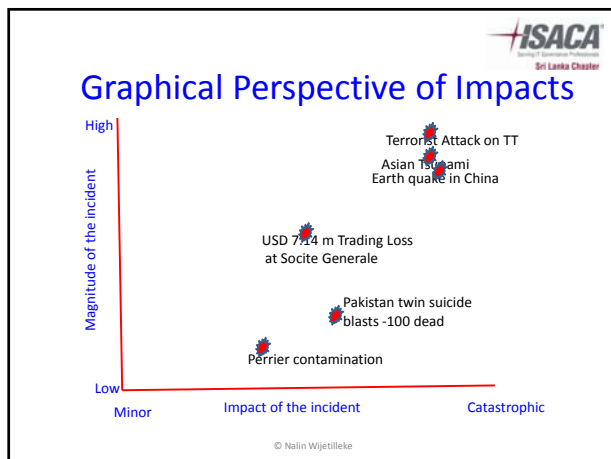


ISACA
Sri Lanka Chapter

Drivers of Business Continuity

- Need for continuous service delivery
- Protection of People and Assets
- Rising vulnerability of materialization of Threats
- Compliance regimen

© Nalin Wijetilleke



ISACA
Sri Lanka Chapter

Scale of a disaster

- Unpredictable
- Destruction of Human Life
- Loss of Property
- Financial Impact
- Impact at
 - Individual level
 - Organizational level
 - Community level
 - National level
 - International level

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Disasters are unpredictable!




Dubai Floods - January 2008

Sri Lanka Central Bank Bombing - January 1996

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Managing Incidences- What do organizations Really Want?



Affordable

Reliable

Comprehensive

Auditable

ISACA
Sri Lanka Chapter

What do we Really Have?

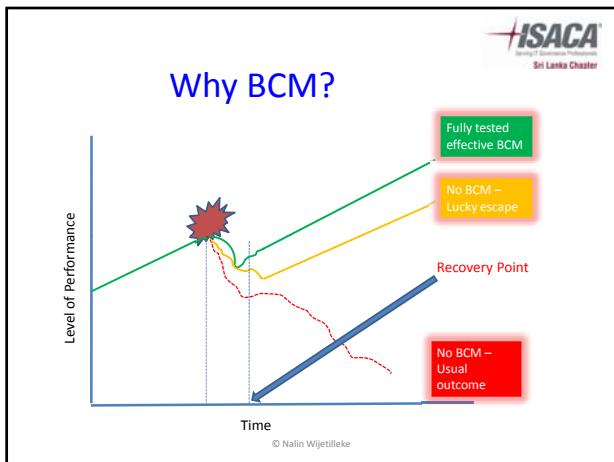


Expensive

Complicated

Inconsistent

Not Auditable



- ### What is the SMART way?
- Doing the RIGHT things and THINGS right
 - Two way process
 - Should be realistic and testable
 - Complete on Time
 - Ongoing Maintenance
- Apply **SMART** business Objectives

- ### Step 1
- Prepare a Business Case
- Contents
- The issue
 - Where are we now?
 - What would be the consequences of a probable crisis or disaster
 - What is therefore our Aim?
 - What would be the initial investment (budget)
 - Who should be responsible?
 - When should we start, when should we finish
- © Nalin Wijetilleke

Investment vs. Risk

Does it justify?

Cost of implementing BCM

Cost of not implementing BCM

“There are risks & costs to a program of action, but they are far less than long range risks and comfortable inaction”. John F Kennedy

ISACA
Sri Lanka Chapter

Management Buy-in

- Who will initiate?
CEO/COO/CFO/CIO/CRO/CIA/Business Head(s)

Remember – it is a Program and not a Project

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Implementing a Business Continuity Management System

- Approaches ?
 - Different approaches are available
 - This presentation suggests BS 25999 route
- Business Continuity Management – Part 1: Code of Practice
 - ✓ BS 25999 -1:2006
- Business Continuity Management – Part 2 : Specification
 - ✓ BS 25999 – 2:2007

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

BS 25999 -2 BCM Standard

- BCM Lifecycle

Ref. BS 25999-1:2006

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

PDCA Model applied to BCM

Ref. BS25999-2 2007 24

© Nalin Wijetilleke

Step 2



Understanding the Organization

- Appointment of a person responsible for BCM implementation
- Develop the BCM Policy
- Conduct a Business Impact Analysis
- Determine your mission critical lines of business

© Nalin Wijetilleke

Business Impact Analysis -BIA



- Aim – To assess over time the impacts that would occur if those activities supporting the delivery of KEY products & services
- How –
 1. Select interviewees
 2. Assess impacts over time, disruption to the activity
 3. Establish MTPOD –Maximum Period of Downtime , RTO – Recovery Time Objective
 4. Identify interdependencies i.e. People, Supporting Infrastructure, resources
 5. Prioritize recovery process & gain consensus

© Nalin Wijetilleke

Business Impact Analysis -BIA

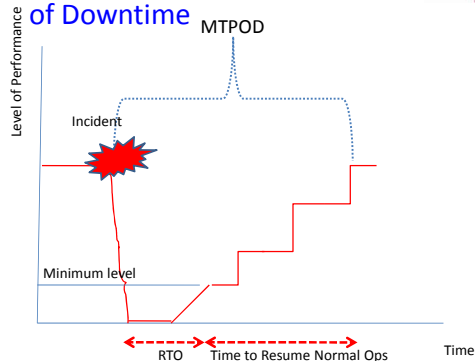


- Example

Sr No	Business Process	Impact of n/a	Minm. level expectation	RTO	Full Sevc. To be within	Other Dependencies
1						
2						
3						
4						
5						
6						
7						

© Nalin Wijetilleke

Maximum Tolerable Period of Downtime



© Nalin Wijetilleke

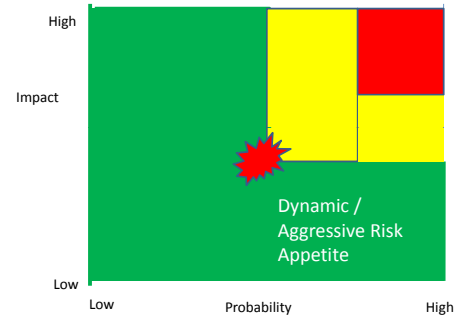
Step 3



- Risk Assessment
 - Determine the criteria of Risk Acceptance
 - Determine the acceptable level of Risk
 - Analyze the Risks & 'to be' position
 - Conduct Gap Analysis for Risk Mitigation

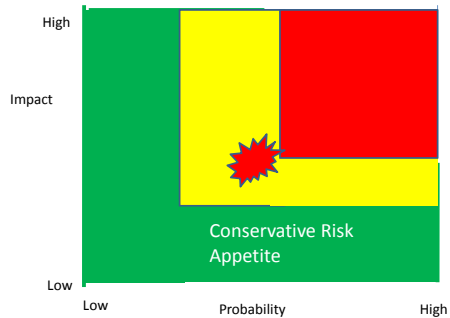
© Nalin Wijetilleke

Risk Appetite



© Nalin Wijetilleke

Risk Appetite



© Nalin Wijetilleke

Step 4



Determine BCM Strategies & Options

As a result of BIA & Risk Assessment the organization should identify measures that

- Reduce the likelihood of a disruption
- Shorten the period of disruption
- Limit the impact of disruption

These are loss mitigation & risk treatment measures

Not All Risk can be prevented or reduced

© Nalin Wijetilleke



BCM Strategies

- Develop Strategies & Options
- Loss mitigation strategies may be used with in conjunction with other strategies
- Business Continuity
 - Acceptance
 - Transfer
 - Change, Suspend or Terminate

© Nalin Wijetilleke



Strategy Options

Strategies might be required for the recovery of following organizational resources

- People
- Physical Infrastructure
- Technical Infrastructure
- Information
- Business Processes (including supplies)
- Stakeholders

© Nalin Wijetilleke



Step 5

Develop and Implement BCM responses

- Develop Response Plans and document
 - Recognizing the incident or potential incident
 - Incident escalation
 - Trigger appropriate BC response
 - Will have resources to support the plan
 - Communicate with the stakeholders

© Nalin Wijetilleke



Components of Emergency Response

- Internal Escalation Procedure
- Emergency notification procedure
- Integrated Response
 - Life Safety Procedures
 - Property Protection/Physical Security
 - Technology Protection
 - Protection of the organization
- Training procedures and responsibilities

© Nalin Wijetilleke

Crisis Management



- Response action at ground level
- Incident Escalation
- Incident Management Framework
- Media Policy & Corporate spokesperson
- Central Command
- Welfare of People
- Continuity & recovery of critical activities

© Nalin Wijetilleke

Step 6

Embedding BCM in the Organization's Culture

- Building, promoting and embedding a BCM culture within an organization ensures that it becomes a part of the organizations core values and effective management

© Nalin Wijetilleke

Building a BCM culture in the Organization

How?

- Leadership of Top Management
- Assignment of roles & responsibilities
- Awareness raising
- Skills development
- Exercising

© Nalin Wijetilleke

Creating Awareness & Training



- Awareness is knowing the reality
- Awareness lead to internalization

- Skills Training
 - Define Training objectives
 - Define Training needs for different user groups
 - Understand the gap
 - Execute
 - Maintain Training records

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Step 7

Exercise, Monitor & Maintain

Ref. BS 25999-1:2006

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Exercise and Test

Testing & Exercising ensures that the BCM arrangements are validated

Testing	Exercising
• Equipment	• People
• Technologies	• Evacuation Procedures
• Durable goods	• Call Tree
• server • ups • generator • telecom	

© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Testing/Exercising as a part of the Plan Life Cycle


© Nalin Wijetilleke

ISACA
Sri Lanka Chapter

Types of Testing

- Table Top
- Walkthrough
- Modular/Component
- Functional
- Simulated
- Comprehensive
- Stress testing
- Surprise

© Nalin Wijetilleke




Step 8

Monitor and Maintain


Maintenance Objective

To evaluate the consistency within the Plan, between the Plan and other aspects of the overall program



Readiness to handle incidences despite Organizational or Environmental Changes

© Nalin Wijetilleke




Monitor and Maintain

- BCM System Review

A review may be triggered by

- Change Management Process
- Exercise or Test
- Internal Audit
- External Audit
- Self Assessment


© Nalin Wijetilleke



Summary

- We are living in a technological world of challenges, uncertainties and turbulence
- Preparedness to uncertainties is better than denial that it would not happen
- Business Continuity Management is a holistic management process that will ensure preparedness
- Readiness to handle incidents should be the main focus, rather than as an audit driven activity

© Nalin Wijetilleke



References:

www.thebci.org

www.drii.org

www.bsi-global.com

Andrew Hills, **Definitive Handbook of Business Continuity Management**, second edition, England: John Wiley & Sons, 2007

© Nalin Wijetilleke



ISACA
Sri Lanka Chapter

PRESS
IN CASE
OF
TROUBLE

Questions ?

nalindw2000@yahoo.com

© Nalin Wijetilleke