Auditing a business continuity management – BCM

November, 2015
Auditing BCM

Agenda

1. Introduction
2. Definitions
3. Standards
4. BCM key elements
Is better to be prepared to a disaster that could never happened, instead, something wrong happens and we are not prepared for it.
Introduction
The need for Continuity Planning

Disasters can strike quickly and without warning,

- Floods, earthquakes, tornadoes, hurricanes, terrorist attacks, …

Business are vulnerable to the impact of not only major calamities but also minor business disruptions,

- Power outages
- IT system failures: v.g. malware or just hacking, Communication failures
- Manufacturing equipment failures
- Hazardous material contamination
- Robbery or other criminal activity
Why are business continuity plans important?

They provide an organized, coordinated and consolidated approach to managing response and recovery activities following any unplanned incident or business interruption, avoiding confusion and reducing exposure to error;

They provide prompt and appropriate response to unplanned incidents, thereby reducing the impacts resulting from short and long-term business interruptions;

They recover essential business operations in a timely manner, increasing the ability of the company to recover from an unplanned incident.
Overall business continuity management

Holistic Approach

- Emergency Response Plan: Focuses on immediate response and life and safety
- Crisis Management Plan: Focuses on strategies and coordination of response
- Pandemic Plan: Focuses on response to outbreak of infectious disease
- Business Continuity Plan: Documents recovery procedures for critical business functions
- Disaster Recovery Plan: Documents procedures for recovery of IT
Overall business continuity management

The general recovery process is illustrated in the next recovery timeline:
Overall business continuity phases

**Phase I**
**Mitigation**
After assessing your risks do what you can to avoid the risk or reduce the impact in case of an emergency or incident.

**Phase II**
**Preparedness**
Be as prepared as you can to minimize the impact in case of an emergency or incident.

**Phase III**
**Response**
Take reasonable actions when emergency or incident occurs.

**Phase IV**
**Recovery**
While still responding, start to think about how to return to normal operations as soon as possible.

Mitigation & Preparedness Occur Before an Incident
Response and Recovery Occur During & After an Emergency
Definitions
Disaster

Is an event, often unexpected, that seriously disrupts your usual operations or processes and can have long term impact on your normal way of life or that of your organization.

- He lost a laptop with the only copy of his thesis
- She lost her research and papers in the lab fire
- Payroll system failed the day before payday
- The death of a employee
- The recent tsunami
- An earthquake
Resilience

Is the ability and capacity to withstand and adapt to new risk environments. A resilient organizations effectively aligns its strategy, operations, business systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks, endure disruptions to its primary earning, drivers and create advantages over less adaptive competitors.

Business resilience does not reduce the likelihood that an event will occur, but it does increase the likelihood that your company will withstand the event.
Definitions

Business Continuity Management - BCM

The goal of BCM is to provide the organization with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organization. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.

According to ISO 22301, a business continuity management system emphasizes the importance of:

- Understanding continuity and preparedness needs, as well as the necessity for establishing business continuity management policy and objectives.
- Implementing and operating controls and measures for managing an organization’s overall continuity risks.
- Monitoring and reviewing the performance and effectiveness of the business continuity management system.
- Continual improvement based on objective measurements.
Definitions

Business continuity Planning

Is a **discipline** that prepares an organization to maintain continuity of business during a disaster through an implementation of a business continuity plan.

A business continuity plan is a **live** document that contains procedures and guidelines to help recover and restore disrupted processes and resources to normal operation status within an acceptable time frame.

It is:

• a process to minimize the impact of a major disruption to normal operations
• a process to enable restoration of critical assets
• a process to restore normalcy to MIT as soon as possible after a crisis.

It is not just: recovery of information technology resources

It is the phase of crisis management that follows the immediate actions taken to protect life and property and contain the event. It begins when the situation has been stabilized.
Definitions
According with ISO 22301:2012

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

**BCP**: documented procedures that guides organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.

**BIA**: process of analyzing activities and the effect that a business disruption might have upon them.
Standards
BCP standards

- BS25999 – British Standard
- ASIS2009: Organizational resilience: security, preparedness, and continuity management systems – requirements with guidance for use
- FSA (Financial Services Authority) – Business continuity management practice guide.
- FFIEC (Federal Financial Institutions Examination Council) – business continuity planning process.
BCP standards

- ISO 24762 (5.11, 5.12, 7.1): provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management.
- ITIL Service continuity management.
- ISO 22301: specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
Key elements
BCP Process

Stage 1: Risk Management

Risk & Controls
Threats, exposures, risk levels, risk controls

Stage 2: Business Impact Analysis

Business Impacts
Critical Processes, Operational & Financial Impacts and Recovery Requirements

Stage 3: Strategy Development

Continuity Strategy
Alternative Critical Resources and Services, and Recovery Methods

Stage 4: BC Plan Development

Documented Business Continuity Plan

Stage 5: BC Plan Testing

Validated Business Continuity Plan

Stage 6: BC Plan Maintenance

Monitor changes and reassesses strategy

Evaluate Test Results

Monitor changes and reassesses risks

Monitor changes and reassesses impacts

Update plan

IT Governance class - IT audit program – BCM – Carlos Garcés – Temple University
BCP Process

**Stage 1: Risk Management**
Assesses the threats of disaster, existing vulnerabilities, potential disaster impacts and identifies and implements controls needed to prevent or reduce the risk of disaster.

**Stage 2: Business Impact Analysis (BIA)**
Identifies mission-critical processes and analyzes impacts to business if these processes are interrupted as a result of a disaster.

**Stage 3: Business Continuity Strategy Development**
Assesses the requirements and identifies the options for recovery of critical processes and resources in the event they are disrupted by a disaster.
BCP Process

Stage 4: Business Continuity Plan Development
Develops a plan for maintaining business continuity based on the results of previous stages (stages 1 to 3)

Stage 5: Business Continuity Plan Testing
Tests the BCP document to ensure its currency, viability and completeness

Stage 6: Business Continuity Plan Maintenance
Maintains the BCP in a constant ready-state for execution
Stage 1: Risk Management

Graphical representation of a risk

Risk

Threat

Possibility of a car accident caused by a drunk driver

AND

Consequences

Expected damage to the car, loss of life, or bodily injury caused by the car accident
Stage 1: Risk Management
Decomposition of the threat components

Risk

<table>
<thead>
<tr>
<th>Threat</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Car accident</td>
</tr>
</tbody>
</table>

Drunk driver

Car accident

Expected damage to the car, loss of life, or bodily injury caused by the car accident
Stage 1: Risk Management
Representation of an example business risk

Risk

Threat

Source

Ice storm

Event

Power outage

Consequences

AND

Expected loss of revenue as a result of the computer center and office facility shut-down: $2.5"
Stage 1: Risk Management
Risk determination

Quantitative Metrics

• Derived algorithmically using probability

• Considerable time and effort are required to gather and analyze data and to explain the results

• Usually you will need historical information

Qualitative Metrics

• Simpler computations (high, medium, low)

• Require less time

• But risk values are subjective and non-repeatable (they are based on judgments)
Stage 1: Risk Management

A risk with quantitative metrics

Risk

- Threat
  - Source: Ice storm
  - Event: Power outage

Consequences

Expected loss of revenue as a result of the computer center and office facility shut-down: $2'5

Risk value: $625,000=

AND

25% probability that a power outage will occur as a result of an ice storm
Stage 1: Risk Management

A risk with qualitative metrics

Risk value: Low

Expected business impact: High

25% probability that a power outage will occur as a result of an ice storm

Risk

Threat

Source

Ice storm

Event

Power outage

AND

AND

Threat

Consequences

25% probability that a power outage will occur as a result of an ice storm
Stage 1: Risk Management Matrix

![Risk Management Matrix Diagram]

- **LOW IMPACT, LOW PROBABILITY**: Ignore
- **LOW IMPACT, HIGH PROBABILITY**: Plan
- **HIGH IMPACT, LOW PROBABILITY**: Normal Procedures
- **HIGH IMPACT, HIGH PROBABILITY**: Change Something
Stage 1: Risk Management

Audit issues

- Scope (processes, facilities, buildings, equipment, technology, human resources, third parties)
- Risk universe used
- Qualification scales (quantitative -- qualitative)
- People interviewed (validation)
- Proper identification and test of controls (D&O – design & implementation, OE – operational efficiency)
- Proper documentation
Stage 2: Business Impact Analysis

Goals

It analyzes the financial and operational impact of disruptive events,

- Financial impact: monetary losses as lost sales, lost funding and contractual penalties
- Operational impact: non-monetary losses as loss of competitive edge, damage to investor confidence, poor customer service, low staff morale, and damage to business reputation

The BIA identifies the following information

- Mission-critical areas of the business and their processes
- Extent of potential operational and financial impact to the organization
- Requirements for recovering disrupted critical business processes

The BIA is a crucial link between the risk management stage and the business continuity plan stage:

- It identifies mission-critical areas and its continuity requirements
Stage 2: Business Impact Analysis

BIA approach

The BIA approach consisted of the four steps outlined below:

1. Identify Business Functions
   - Defined Client function targeted in scope of BIA
2. Collect and Validate Data
   - Conducted BIA kickoff, BIA sessions and Follow Ups
   - Obtained existing documentation including previously established BCPs, BIAs, process flow diagrams.
3. Analyze Data
   - Collected BIA data for scope business processes
   - Requested & received validation/approval of all data captured
   - Analyzed business process MTPD’s
   - Analyzed & aggregated quantitative and qualitative impacts
   - Analyzed internal and external (Third dependencies)
4. Develop BIA Report
   - Developed a formal BIA report
   - Summarized the BIA data
   - Consolidated raw BIA data tables
   - Identified personnel, equipment/supplies requirements
Stage 2: Business Impact Analysis
Recovery Time Requirements

MTD (Maximum Tolerable Period of Disruption)
• Maximum downtime the organization can tolerate for a business process

RTO (Recovery Time Objective)
• Indicates the time available to recover disrupted systems/resources

RPO (Recovery Point Objective)
• It refers to the extent of data loss measured in terms of a time period that can be tolerated by a business process

WRT (Work Recovery Time)
• It’s the time available to recover the lost data, work backlog and manually captured data once the system / resources are recovered or repaired
Stage 2: Business Impact Analysis
Business Terms versus IT Terms

• Terms that start with “M” represent business facing timing parameters
• Terms that start with “R” represent IT facing timing parameters

Key terms for any organization

• Maximum Tolerable Period of Disruption (MTPD)
• Recovery Time Objective (RTO)
• Recovery Point Objective (RPO)
Stage 2: Business Impact Analysis

Disaster-recovery time frame

- **RPO** (Recovery Point Objective)
- **RTO** (Recovery Time Objective)
- **WRT** (Work Recovery Time)
- **MTPD** (Maximum Tolerable Production Down Time)

- **Lost Data**
- **Work Backlog**
- **Collect Data Manually**
- **Recover Work Backlog**
- **Recover Lost Data**
- **Recover Manually Collected Data**

- **Normal Procedures**
- **Emergency Manual (Work-around) Procedures**
- **Manual and Normal Procedures**

- **Last Backup**
- **Disruptive Event**
- **System / Resources Recovered**
- **Start of Normal Processing**
Stage 2: Business Impact Analysis
BIA input and output information

BIA Input

- Business Functions & Processes
- IT and non-IT Resources
- Work-around Procedures

BIA Output

- Mission-critical Business Processes
- Financial and Operational Impact Levels
- Recovery Time Requirements
- Recovery Priorities
- Internal and external Dependencies
- Resource Dependencies
- Critical Process Work-around Procedures
- Summarized Findings
Stage 2: Business Impact Analysis

Audit issues

- Scope (processes, facilities, buildings, equipment, technology, human resources, third parties)
- Qualification scales (quantitative -- qualitative)
- People interviewed (validation)
- Identification of key processes / requirements
- Are the mission-critical business processes according with the business needs / requirements? What is the rationale of it? The process followed to obtain it, is well done?
- Are the RTO, RPO and MTPD right according with the business needs / requirements? The process followed to obtain it, is well done?
- Are logical the estimation of the financial and operational impact levels? Are these estimates according with the business needs / requirements? The process followed to obtain it, is well done?
Stage 2: Business Impact Analysis

Audit issues

• The recovery priorities are based on the needs and requirements of the enterprise?
• Has been identified the main resources for each critical processes?
• Has been identified all the main internal and external dependencies?
• Has been identified and documented all the critical process work-around procedures?
• Proper documentation
Stage 3: strategy development

Begin BC Strategy Development Phases

**Step 1:** Identify Recovery Requirements

**Step 2:** Identify Work Area Recovery Requirements
- Office Work Area
- Crisis Management Center
- Work Area Recovery Options

**Step 3:** Identify IT Systems & Infrastructure Recovery Requirements
- Alternate IT Recovery Facilities
- Critical IT Systems & Production Facilities
- IT Systems & Infrastructure Options

**Step 4:** Identify Manufacturing & Production Recovery Requirements
- Alternate Manufacturing & Production Facilities
- Critical Equipment & Resources
- Manufacturing & Production Options

**Step 5:** Identify Data & Critical/Vital Records Recovery Requirements
- Critical Data
- Critical Vital Records
- Data & Critical/Vital Records Recovery Options

Assess Available Time of Options against Recovery Time Requirements

**Step 1:** Select Capability Requirements

**Step 2:** Evaluate Recovery Options

**Step 3:** Select Viable Recovery Options

Business Continuity Strategy
Stage 3: strategy development
Match the tools to the business needs
Stage 3: strategy development
Process / functions strategies

- Alternative functional work-area recovery strategies aligned with RTO.

<table>
<thead>
<tr>
<th>Pre-Staged Workspace</th>
<th>Commercial Work-Area</th>
<th>Dedicated Workspace</th>
<th>Remote Access</th>
<th>Mobile Facility</th>
<th>Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated Facility &amp; Infrastructure Providing Immediate Access to a Replicated Work Environment</td>
<td>Shared Vendor Facility Permitting Rapid Access to Workspace, PC’s, Equipment &amp; Voice Applications</td>
<td>Dedicated Facility Requiring Quick-Shipment of Desktop PC’s, Office Equipment &amp; Infrastructure</td>
<td>Vendor Facility Shipped to Your Location and Configured for Rapid Setup and Population</td>
<td>Best Effort At Time of Disruption to Acquire Class-A Office Space</td>
<td></td>
</tr>
</tbody>
</table>

Continuum of Process/Function Availability Strategies

Cost of Solution

Time To Operational Availability

- Minutes
- Hours
- Days
- Weeks
Stage 3: strategy development
Application availability strategies

- Alternative IT application recovery strategies aligned with RTO.
Stage 3: strategy development
Application data recovery strategies – selection criteria

- Alternative electronic application data recovery strategies aligned with RPO.

![Continuum of IT Application Data Recovery Strategies](image-url)
Stage 3: strategy development

Vital record recovery strategies – selection criteria

- Alternative physical vital record recovery strategies aligned with RPO.

Continuum of Vital Record Recovery Strategies:

- Manual Recreation
- Fire-Proof Storage
- Manual Relocation
- Facsimile Relocation
- Electronic Imaging
- Electronic Replication
- Records Scanned into an Electronic Image for On-Line Replication to Off-Site Storage
- Records Scanned into an Electronic Image for Periodic Bulk Data Transfer to Off-Site Storage
- Record Facsimile Transmitted Electronically via Public Telephone Network to Off-Site Storage

Chronological Point in Time For Record Recovery:

- Weeks
- Days
- Hours
- Minutes

Cost of Solution:

- $$$
Stage 3: strategy development

Audit issues

• Are the strategies aligned with the RTO / RPO?
• How was the strategy’s costs estimated?
• Are the strategies aligned with the management goals?
• Are the strategy’s costs well balanced with the amount of the loss?
• Are the strategies easy to maintain, easy to test, easy develop, let to operate for a long time?
• Are the strategy’s selection made by the management?
• Proper documentation
Stage 4: Plan development

Phases

- **Phase 1:** Initial Response & Notification
- **Phase 2:** Problem Assessment & Escalation
- **Phase 3:** Disaster Declaration
- **Phase 4:** Plan Implementation & Logistics
- **Phase 5:** Recovery and Resumption
- **Phase 6:** Normalization

**Disaster / Disruptive Event**

- Results in a Preliminary Problem Report
- Results in a Detailed Problem Report
- Results in a Disaster Declaration Statement
- Results in Mobilization of Teams, Backup Media and Critical Resources and Equipment
- Results in Recovery of Critical IT and Non-IT Resources and Processes
- Results in Pre-disaster Operational Status

IT Governance class - IT audit program – BCM – Carlos Garcés – Temple University
Stage 4: Plan development
Incident escalation

Incident

Incident Management Team and CMT informed

Assess severity and respond as appropriate

Major severity (Crisis)

CMT informed and activated

CMT meet and agree actions

Crisis resolved

Invoke and activate the BCPs

No

Yes

Post crisis report produced

Incident closed

Yes

Incident resolved

Manage incident at op. level

Minor severity

Yes

Incident closed

CMT informed and activated

No

Incident closed

Incident Management Team and CMT informed

Assess severity and respond as appropriate

Crisis resolved
Stage 4: Plan development

Components

- BCM Policies
- Recovery teams (crisis management team, incident management team, crisis communication team, DRP management team, BCP’s teams)
- Governance (BCP leader, DRP Leader)
- Roles and responsibilities (normal and disaster time)
- Key performance indicators (defined and measurement)
- BCP directory (address, cell phone, phone) – internal and external
- Call tree
Stage 4: Plan development

Audit issues

- Are the BCM policies approved by the management?
- Are the incident escalation according with the company’s needs and requirements?
- Is properly defined the procedure to share the information of the call tree and directory?
- Are the BCM’s, BCP’s and DRP's leaders properly defined according with the skills and knowledge of the people selected?
- Are the teams well structured?
- Are properly defined the spokesmen?
- Proper documentation
Stage 5: Testing
Testing scheme

Test Complexity

High
Medium
Low

Test Schedule

Monthly
Quarterly
Semi-annually
Annually

Walkthrough
Checklist
Simulation
Full-interruption
Unannounced

Complexity

Low
Medium
High
Stage 5: Testing

Audit issues

- Are the BCM’s components properly tested?
- Is the BCM’s test process properly defined and approved?
- Is the test frequency properly defined?
- Each test has its own data set and time and results expected?
- After each test, the results are analyzed and a work plan is defined to solve the problems presented?
- Is there a follow up to the implementation of the work plan? Who is the responsible?
- Are the strategies aligned with the RTO / RPO?
- Is the test program cumulative?
- Proper documentation
Stage 6: Plan maintenance

Audit issues

Step 1: Monitor Internal & External Changes

Step 2: Compiled Changes

Step 3: Review Compiled Changes & Results of Plan Test & Audits

Periodic BC Plan Testing

Test Results

Audit Results

Periodic BC Plan Audit

BC Plan Change Request

Process BC Plan Change Request

Revised Bc Plan Document
Stage 6: Plan maintenance

Audit issues

• Is the BCM’s plan maintenance properly defined and approved?
• Are identified the activities that causes bcp changes / modifications?
• Is defined the internal and external BCP audit program?
• Is clear who is the responsible(s) to update the BCP?
• Proper documentation
Thank you