CoBIT 5: Managing Continuity Aspects
With A Practical Approach

Amardeep Singh
Business Continuity Consultant

ISACA Adelaide Chapter
12 May 2015
Discussion

• Business Continuity Management (BCM)
• Standards and Best Practice
• CoBIT 5 & BCM: Practical Implementation
• Future Trends
• Information Sharing
## CoBIT 5 & Managing Continuity

### Chapter 5

#### COBIT 5 Process Reference Guide Contents

<table>
<thead>
<tr>
<th>DSS04 Manage Continuity</th>
<th>Area: Management Domain: Deliver, Service and Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Description</strong></td>
<td>Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.</td>
</tr>
<tr>
<td><strong>Process Purpose Statement</strong></td>
<td>Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.</td>
</tr>
<tr>
<td>The process supports the achievement of a set of primary IT-related goals:</td>
<td></td>
</tr>
<tr>
<td><strong>IT-related Goal</strong></td>
<td><strong>Related Metrics</strong></td>
</tr>
</tbody>
</table>
| 04 Managed IT-related business risk | • Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment  
• Number of significant IT-related incidents that were not identified in risk assessment  
• Frequency of update of risk profile |
| 07 Delivery of IT services in line with business requirements | • Number of business disruptions due to IT service incidents  
• Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels  
• Percent of users satisfied with the quality of IT service delivery |
| 14 Availability of reliable and useful information for decision making | • Level of business user satisfaction with quality and timeliness (or availability) of management information  
• Number of business process incidents caused by non-availability of information  
• Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor |

Source: CoBIT 5
International Standard 22301 Definition

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

Or Simply

“continuing business in times of a threat / s”
“safety”
“criticality”
Threats: Natural and Man Made

Source: www.bom.gov.au


Source: www.nbcnews.com

Source: www.skynews.com.au

Source: www.northlandsnewscenter.com/home/PIN-numbers-also-part-of-Target-data-breach-237547411.html

Source: The Australian

Australian terror alert level raised to high

Updated: 4:13 pm, Friday, 12 September 2014
Source: www.skynews.com.au

Human error triggered NAB software corruption

Source: The Australian
<table>
<thead>
<tr>
<th></th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Damage to reputation/brand</td>
</tr>
<tr>
<td>2</td>
<td>Economic slowdown/slow recovery</td>
</tr>
<tr>
<td>3</td>
<td>Regulatory/legislative changes</td>
</tr>
<tr>
<td>4</td>
<td>Increasing competition</td>
</tr>
<tr>
<td>5</td>
<td>Failure to attract or retain top talent</td>
</tr>
<tr>
<td>6</td>
<td>Failure to innovate/meet customer needs</td>
</tr>
<tr>
<td>7</td>
<td>Business interruption</td>
</tr>
<tr>
<td>8</td>
<td>Third-party liability</td>
</tr>
<tr>
<td>9</td>
<td>Computer crime/hacking/viruses/malicious codes</td>
</tr>
<tr>
<td>10</td>
<td>Property damage</td>
</tr>
</tbody>
</table>

Impacts

Insured losses from disasters below average in 2014 despite record number of natural catastrophe events, says Swiss Re sigma study

25 MARCH 2015, ZURICH

- Total global economic losses from natural catastrophes and man-made disasters were around USD 110 billion in 2014
- This compares to global insured losses of about USD 35 billion in 2014, below the USD 64 billion-average of the last 10 years
- There were 189 natural catastrophes worldwide last year, the highest on sigma records
- Disasters claimed more than 12 700 lives in 2014, one of the lowest ever in a single year
- Severe thunderstorm losses are trending upward – details in the special chapter of this sigma


Figure 1: Number of disasters events, 1970–2014

Source: Swiss Re Economic Research & Consulting and Cat Perils.
Benefits of BCM

- Prepare: Safety, Insurance advantages
- Reduces risk of damage and access vulnerabilities
- Safely continue during “threat” conditions (keep business running)
- Data loss and recovery times minimised
- Regulatory and Governance (who is responsible for BC?)
- Competitive advantage – reputation, certified

Evidence that firms do not invest enough time and resources into BCP preparations are evident in disaster survival statistics. Fires permanently close 44% of the business affected. In the 1993 World Trade Center bombing, 150 businesses out of 350 affected failed to survive the event. Conversely, the firms affected by the Sept 11 attacks with well-developed and tested BCP manuals were back in business within days.

Early Years (60s and 70s)

1969: Information Security Audit and Control Association (ISACA)

1980s: ITIL (British Govt)

1988: DRI International (DRII) – Professional Practices (US)

1994: Business Continuity Institute (BCI) – GPG (UK)

2006: BS 25999 Business Continuity Management

2009: Australian National Audit Office (ANAO)

2012: ISO Standard 22301

2012: CoBIT 5

BS 65000 Guidance on Organizational Resilience
Other Standards / Guides

• Australian Prudential Regulatory Authority (APRA)
  • APS 232: Business Continuity Management (deposit institutions)
  • GPS 222: Business Continuity Management (insurance)
  • CPS 232: Business Continuity Management (Board of Directors or equivalent have ultimate responsibility)
• AS/NZS 5050:2010: Business continuity – Managing disruption-related risk

Sources (Slides 11 -14, 16 – 21):
Good Practice Guidelines 2013 v3.1 (BCI 2013)
CoBIT5: Enabling Processes (ISACA 2012)
## ISACA CoBIT 5: Continuity Related Practices

| Key Management Practice                                      | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy, Executive Committee | Steering (Programmes/Projects) Committee | Portfolio Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---------------------------------------------------------------|-------|-------------------------|-------------------------|------------------------|----------------------|-----------------------|---------------------------|-------------------------------------|------------------------------------------|----------------------------|-----------------|-----------------|----------------------------------|-------------------|-----------------------|---------------------|-------------|------|-------------------------|-----------------|---------------------|--------------------|----------------|--------|------------------------|-----------------|---------------------|
| DSS04.01 Define the business continuity policy, objectives and scope. | A     | C                       | R                       |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.02 Maintain a continuity strategy.                     | A     | C                       | R                       |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.03 Develop and implement a business continuity response. | I     | R                       |                          |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.04 Exercise, test and review the BCP.                  | I     | R                       |                          |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.05 Review, maintain and improve the continuity plan.    | A     | I                       | R                       |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.06 Conduct continuity plan training.                   | I     | R                       |                          |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.07 Manage backup arrangements.                        |       |                          |                          |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
| DSS04.08 Conduct post-resumption review.                     | C     | R                       | I                       |                        |                      |                       |                           |                                     |                           |               |                |                                   |                   |                       |                     |             |      |                         |                 |                     |                     |               |        |
Professional Practices (PP)

Management Practices
- Policy and Programme Management
- Embedding Business Continuity

Technical Practices
- Analysis
- Design
- Implementation
- Validation
CoBIT & GPG: Policy / Governance

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs From</th>
<th>Inputs Description</th>
<th>Outputs Description</th>
<th>Outputs To</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS04.01 Define the business continuity policy, objectives and scope. Define business continuity policy and scope aligned with enterprise and stakeholder objectives.</td>
<td>AP009.03</td>
<td>SLAs</td>
<td>Policy and objectives for business continuity</td>
<td>AP001.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Disruptive incident scenarios</td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assessments of current continuity capabilities and gaps</td>
<td>Internal</td>
</tr>
</tbody>
</table>

- Policy and Programme Management (PP1) is at the start of the Business Continuity Management (BCM) Lifecycle. It is the Professional Practice that defines the organizational policy relating to Business Continuity (BC) and how that policy will be implemented, controlled and validated through a BCM programme.

Practical

- Other priorities, Buy In
- Where start, what and who covered?
- Who will do this?

Solutions

Project Management (Cost vs Benefit) Responsibilities

Experts Communication

May 13, 2015
CoBIT & GPG: Analysis and Design

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSS04.02 Maintain a continuity strategy.</strong> Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption.</td>
<td><strong>From</strong> AP012.06 <strong>Description</strong> • Risk-related root causes • Risk impact communications</td>
<td><strong>Description</strong> Business impact analyses AP012.02 <strong>To</strong> Continuity requirements Internal Approved strategic options AP002.05</td>
</tr>
</tbody>
</table>

**Analysis (PP3)**

is the Professional Practice within the BCM Lifecycle that reviews and assesses an organization in terms of what its objectives are, how it functions and the constraints of the environment in which it operates.

**Design (PP4)**

is the Professional Practice within the BCM Lifecycle that identifies and selects appropriate strategies and tactics to determine how continuity and recovery from disruption will be achieved.

**Practical**

- Priorities and political - criticality
- What and who covered?
- Who will do this and how?
- Alignment and changes

**Solutions**

Senior Management Prepare

Tools Experts Reuse / Share
BC and Alignment (DR - IT)

Disaster Declared

Management decision to invoke

Disaster Alert Notification

Damage Assessment

Disaster Declaration Assessment

Manual Workarounds

Resumption of CRITICAL services

Business activities

Technical Recovery Time Objective (RTO)

Service Interruption

Recovery Point Objective (RPO)

Maximum Tolerable Period of Disruption (MTPD)

New site, same site, other, backlog

Source: CSC, Business Continuity Services
CoBIT & GPG: Implementation

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS04.03 Develop and Implement a business continuity response.</td>
<td>From</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>AP009.03</td>
<td>OLAs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident response actions and communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DSS02.01</td>
</tr>
</tbody>
</table>

• Implementation (PP5) is the Professional Practice within the Business Continuity Management (BCM) Lifecycle that executes the agreed strategies and tactics through the process of developing the Business Continuity Plan (BCP).

Practical

- Size (Strategic, Tactical, Operational, 1)
- Responsibilities - Criticality
- Simple - Useful

Solutions

<table>
<thead>
<tr>
<th>Organisational Knowledge</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reuse / Share</td>
<td>Validate</td>
</tr>
</tbody>
</table>
### CoBIT & GPG: Validation (Exercise, Test, Review)

**DSS04.04 Exercise, test and review the BCP.**
Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.

<table>
<thead>
<tr>
<th>From</th>
<th>Description</th>
<th>Description</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Test objectives</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Test exercises</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Test results and recommendations</td>
<td>Internal</td>
<td></td>
</tr>
</tbody>
</table>

**Validation (PP6)**

is the professional practice within the BCM Lifecycle that confirms that the BCM Programme meets the objectives set in the BC Policy and that the organization's BCP is fit for purpose.

### Practical

- Other priorities
- Relevance & Regularity (how)
- Who (does this, involved)

### Solutions

<table>
<thead>
<tr>
<th>Planning Cycle</th>
<th>Report</th>
<th>Follow up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experts</td>
<td>Contracts</td>
<td>Tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planning (3 years)</td>
</tr>
</tbody>
</table>
CoBIT & GPG: Validation (Review, Maintain, Improve)

Management Practice
DSS04.05 Review, maintain and improve the continuity plan.
Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up to date and continually reflects actual business requirements.

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Validation (PP6)
is the professional practice within the BCM Lifecycle that confirms that the BCM Programme meets the objectives set in the BC Policy and that the organization’s BCP is fit for purpose.

Practical
• Benchmark & Audits
• Relevance & Regularity (how)
• Who (does this, involved)

Solutions
Planning (3 years) Responsibilities Performance (KRA)
Tools Organisation Daily Tasks (Change, Release) & Culture
CoBIT & GPG: Awareness

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS04.06 Conduct continuity plan training. Provide all concerned internal and external parties with regular training sessions regarding the procedures and their roles and responsibilities in case of disruption.</td>
<td>HR</td>
<td>Training requirements, AP007.03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring results of skills and competencies, AP007.03</td>
</tr>
</tbody>
</table>

**Practical**

- Regularity
- Who (does this, involved)
- Costs

**Solutions**

Planning (3 years) Lead – Senior Management

Use “Threats” & “Opportunities” (BCAW) Experts
## CoBIT & GPG: Backups

### Management Practice

<table>
<thead>
<tr>
<th>DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

### Activities

1. Back up systems, applications, data and documentation according to a defined schedule, considering:
   - Frequency (monthly, weekly, daily, etc.)
   - Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention)
   - Type of backup (e.g., full vs. incremental)
   - Type of media
   - Automated online backups
   - Data types (e.g., voice, optical)
   - Creation of logs
   - Critical end-user computing data (e.g., spreadsheets)
   - Physical and logical location of data sources
   - Security and access rights
   - Encryption

### Solutions

#### Relevance (BIA)

- Practical
  - Costs - Criticality
  - Protect

#### Senior Management Directive
CoBIT & GPG: Never Ends

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS04.08 Conduct post-resumption review. Assess the adequacy of the BCP following the successful resumption of business processes and services after a disruption.</td>
<td>From</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To</td>
</tr>
<tr>
<td>Post-resumption review report</td>
<td></td>
<td>Internal</td>
</tr>
<tr>
<td>Approved changes to the plans</td>
<td></td>
<td>BAI06.01</td>
</tr>
</tbody>
</table>

Practical & Solutions

- DSS04.01 to DSS04.07
- PP1 to PP6
- Backlog Planning
Future Trends: New Developments; New Threats

Challenge

• Business / Client Demands
• Technology – Cloud, Big Data, Social Media, Mobility
  Internet of Things {IoT}
• Natural and Man Made threats simultaneously and higher occurrence

Solutions

• Update skills
• Multi tasking
• Networking
• Think outside the square
• Experts
• Communication

Ebola Outbreak: Why Pandemic Prep Matters

As the current Ebola outbreak in West Africa spreads, organizations across the world have a grim reminder that pandemic preparedness and response should be a priority in their emergency planning.

Source: DRII Newsletter
Summary

- BCM is a holistic approach
- Every organisation is different
- Get Senior buy in up front (responsibility rests here)
- Plan
- Exercise and Test
- Regular and continuous
- Keep up to date
- Resilience
Information Sharing & Further Reading

• Question and Answers
• Share Your Experience
• Further Reading
  • BCI: www.thebci.org
  • CoBIT: www.isaca.org
  • DRII: www.drii.org
Thank You

asingh309@csc.com
csc.com.au