Measuring Continuity Planning Program Performance

Carl B Jackson
Director
Crisis Management & Continuity Planning Resource Center (CMCPRC)

Measuring Continuity Planning Program Performance Session Agenda

• How an enterprise-wide BCP program should be structured…
  – Business Continuity and Crisis Management Process Overview

Two approaches to building metrics processes…

  – Utilizing and Enterprise Risk Management Approach – Value Driver Based
  – Utilizing the ISO 27001 Information Security Management System – Standards Based

Metrics Program Benefits and Recommendations
Metrics Development Approach 1 -
Base metrics on Enterprise Value Drivers
Examples of Value Drivers

- **Customer Satisfaction**
  - Impact on external customers
  - # of customers impacted
  - Duration of impact

- **People**
  - Loss/ access to private employee information
  - Workforce endangerment
  - Access to executive information, systems, etc

- **Financial**
  - Cost Increase
  - Revenue loss

- **Intangible**
  - Proprietary information
  - Damage to brand
If you can't measure it, you don't know it...

1. Identify/Monitor Enterprise Value Drivers
   - Financial
     ✅ Increase sales 10%
     ✅ Decrease expenses 8%
   - Customer Service
     ✅ Increase customer privacy
     ✅ Increase customer service efficiency

2. Define Value Driver Linkages to Program Components
   - Financial
     - Business Impact Assessment Process (drives down expenses due to increased BCP efficiencies)
   - Customer Service
     - Recovery strategy deployment (redundant solutions provide additional bandwidth)

3. Define Metrics for Linked Components
   - Financial
     - BIA updated annually
     - BCP quality survey demonstrates percentage increase in awareness
   - Customer Service
     - Customer service survey demonstrates higher levels of approval
     - Customer wait time decreased by 13%

Metrics Development Time Line

Phase 1/4
1. Identification of Value Drivers

Phase 2/5
2. Map Value Drivers to BCP Process Components
3. Develop Qualitative & Quantitative Metrics for linked components
4. Monitor/Modify Value Drivers
5. Map Value Drivers to BCP Process Components

Phase 3/6
6. Develop Qualitative & Quantitative Metrics for linked components
Executive Management motivation data gathering
(customer satisfaction, financial, intangible, etc.)

Categorize Continuity Program Measurement Components

BCP Lifecycle Components
(BIA, Emergency response Procedures, Crisis Management Teams, Documented Plans, Test Plans, Training, etc.)

Examples could include:
- Timely business impact assessments are performed
- The Continuity Planning infrastructure was developed utilizing a methodological approach
- Emergency Response Procedures are:
  - Formalized
  - Address life safety considerations of both employees and outsiders
  - Located or posted in conspicuous locations throughout each facility
  - Operating personnel have received training within the past six months
- Emergency Response Procedures are tested periodically (at least semi-annually)
- Emergency Response actions are coordinated with Civil Authorities, internal facilities management, etc.
- Updated at least semi-annually
- Auditable and audited with no resulting significant criticisms

Metrics Development Approach 2 –
Base metrics on commonly recognized standards and practices (ISO 27001 for instance)
ISO 17799/27001 Scope

• ISO 17799 (should) is an International Standard that provides:
  – recommendations for Information Security Management (133 control objectives)
  – a common basis for developing organizational security standards and effective
    security management practices
  – confidence in inter-organization dealings
  – an organization cannot get certified against ISO 17799

• ISO 27001 (shall) is an International Standard that provides management
  guidelines for implementing and managing the 133 control objectives utilizing
  a coordinated Information Security Management System (ISMS) approach:
  – When properly implemented the ISMS provides auditable and certifiable proof as to
    the effectiveness of the ISMS and the 133 control objectives
  – ISO 27001 assists us in ‘how we manage’ information security for auditability and
    certification

Base Standards on ISO27001

BCP Requirements

• ISO27001 Aspects of the Business Continuity Management Program
  ▪ Business Continuity Management Process – Business continuity management
    processes shall be established to ensure uninterrupted of business activities.

  ▪ Business Continuity and Impact Analysis – A comprehensive risk management
    process shall be applied to business processes

  ▪ Writing and Implementing Continuity Plans – Business continuity plans shall ensure
    maintenance or timely recovery of business activities

  ▪ Business Continuity Planning Framework – Business continuity plans shall have a
    single framework to facilitate the testing and review of plans

  ▪ Establish Testing, maintenance, and assessments for business continuity plans
ISO27001 BCP Framework

Executive Policy Statement (Info Sec, Phy. Sec., BCP, etc.)

Business Continuity Program - Charter

Business Continuity Program – Enterprise Standards/Processes

• Operating Area Specifications
• Operating Area Procedures
• Operating Area BCP Testing

BCP Program Framework

• BCP Policy & Charter
  - Governance
  - Scope
  - Roles & Responsibilities
  - Company Objectives
  - The “WHY”

• BCP Standards/Processes
  - Baseline Requirements
  - Enterprise-Wide Synergy
  - Repeatable Processes
  - Consistency/Predictability
  - The “WHAT”

• BCP Specifications
  - Operating Area Established
  - Operating Area Maintained
  - Operating Area Defined Metrics
  - The “HOW”

  • Legislative / Regulatory Compliance
  • Executive Management Direction
  • Enterprise-Wide Due Diligence
  • Competitive Advantage
  • ISO 27001 Alignment
  • Predictable/Repeatable
  • Industry Best Practices
BCP Framework - Gap Analysis

- **Gap Analysis Process**
  - Same Process as ISMS
- **Alignment with Standards**
  - Operating Area Specifications
  - Operating Area Procedures
- **Gap Remediation**
  - Critical and Highs
  - Remediation Plans
- **Gap Acceptance**
  - Formal Process & Signoffs
- **Measurement**
  - Test Objectives vs. Results
Benefits of Metrics

- Can be used to reduce costs (*insurance possibly*)
- Can be used as an advantage in the marketplace
- Provides a map to where process improvement may be needed
- Provides oversight insight (*audit, compliance*)

Recommendations

- Think in terms of how do you as a planner get management attention, buy-in and budget?
  - One way is to develop and be measured against a set of metrics.
- How do you as a Continuity Planner demonstrate the value-add contributions of the enterprise continuity planning business process?
- Stay out of the weeds – Don’t focus on IT recovery only – THINK “Value-add contribution to the business/mission” or “Adherence to standards through periodic gap analysis.”
- Focus on defining who the stakeholders are (corporations -shareholders, government-the people)
  - What does the key stakeholder value from this organization?
- Break the BCP process down so we can make operational, manageable, and measurable decisions.
- Discuss and present in Executive Management terminology.