Business Continuity Management
An Internal Audit Perspective

January 14, 2015
Tony Adame
Director Of Consulting Services
Ripcord

- Responsible for providing business continuity planning, emergency response planning, IT disaster recovery, and crisis management services to Ripcord clients.
- 20 years experience in BCM across many industries – both internal and external resource.
- Designed and led tabletop and hot-site exercises for numerous clients in numerous industries.
- Facilitated real-time Business Continuity, IT Security, and IT DR responses to major incidents.
- Started career as an Internal Auditor.
Two Quick Audit Stories

1993 Avco Financial Services

2012 an Unnamed Credit Union
Why audits/assessments are initiated.
Understand major areas of BCM programming that auditors (examiners) should be interested in reviewing.
Outline various audit/compliance rules, regulations, guidelines available to investigative personnel.
Discuss methods to gather information to examine.
Better understand what auditors and regulators should be trying to accomplish by your assessment.
Discuss ways to use an assessment to grow and mature the company’s resiliency programming.
How many of you have completed an audit of a company’s BCM program?

Of those, how many were anxious about how to build a scope and the eventual results?

Did you feel competent and qualified to conduct the review (conversely did you have to learn what BCM was beforehand)?

What was the best part of the review?

What was your least favorite part of the process?

Did any real good come out of it?
What Are the Threats We Face?
What Triggers an Audit

- Recent Incident (local, regional, industry or company specific)
  - NOTE: Beware of “rabbit holes” e.g., Black Swan events.
- Budget Analysis
- Board Level Interest (Audit Committee)
- Regulatory Compliance
- Known Weakness in One or More BCM Components
- Holding Company Directive
- New Senior Leadership
- Client or Regulator Inquiry
- BCM Coordinator Ask
- External Auditor Request
- Others??
Various Rules, Regulations, Standards, & Guidelines

- ISO 22301
- FFIEC – (Banking Compliance)
- PS Prep (Public Private Resiliency Certification)
- Dodd-Frank (Banking)
- SEC Rule 33-9089 (Corporate Enterprise Risk Mgmt)
- NCUA – Letter #8 (Credit Union)
- COBIT (IT Disaster Recovery)
- ANSI/ARMA 5-2003 Vital Records Programs (Records Mgmt & Retention)
- HIPAA (Patient Privacy & Records Recovery)
- California 8 CCR Section 3220 (Emergency Response)
- Joint Commission (Healthcare Emergency Response)
- NRS 463.790 (Nevada Resort and Casino Emergency Response)
- Calif. SB 1386 (Citizen Personal Privacy)
Business Continuity Management

The advance preparations necessary to identify the impact of potential business interruptions; formulate recovery strategies; develop business continuity plans; and administer a training, exercise and maintenance process.

An organization's coordinated, effective and timely response to an emergency. The goal is to avoid or minimize injury to personnel and/or damage to company assets.

The technological tenets of a business continuity program. Focus is on restoration, possibly at an alternate location, of data center services and computing capabilities.

The ability to strategically manage an event including the internal and external communications necessary to protect corporate reputation and brand image.

An organization's coordinated, effective and timely response to an emergency. The goal is to avoid or minimize injury to personnel and/or damage to company assets.

The process to identify risk and quantify impact to the business (people, operations, finances etc.)
What You Should Want To Know

- Does senior management provide sufficient resources and oversight to the BCM Program?
- Is there integration between the various response and recovery plans (ERP, CM, IT DR & BCP)?
- Is the BCM Coordinator qualified to oversee the Program?
- Have threats been identified and quantified?
- What mechanisms are in place to mitigate threat impacts?
- Are employees and facilities protected?
- Can IT recover key infrastructure and application assets in a timely manner after an event?
What You Should Want To Know – cont’d

- Can executives communicate as a team?
- Have mission-critical processes been identified?
- How long can the operations be down?
- What are the financial, operational, reputational, and compliance impacts resulting from a disruption?
- What resources will be needed after an event?
- Are plans in place to continue operations absent facilities, IT, key personnel &/or critical vendors/business partners?
- Have plans been exercised?
- Do all pertinent personnel understand their role in the company’s resiliency efforts?
- What long-term maintenance procedures exist?
Key Areas of Analysis

- Risk Assessment complete and current
- Sr. Leadership, IT and business coordinated
- Communication (Identification, Notification, & Escalation)
- Current and approved BIA
- RTOs and RPOs defined and quantified
- IT Gap Analysis available
- Tactical ERP, CMT, IT DR & BCP integration & hand offs
- Growth & maturity over time

The committee is multi-disciplinary and involves participants from both the public and private sectors.

The committee develops standards for the protection of society from, and in response to, incidents caused by intentional and unintentional human acts, natural hazards and technical failures.

Its all-hazards perspective covers adaptive, proactive and reactive strategies in all phases before, during and after a disruptive incident.
Focus on ISO 22301 : 2012

- Applies to all types and sizes of organizations that wish to:
  - establish, implement, maintain and improve a BCM Program;
  - assure conformity with the organization’s stated business continuity policy;
  - demonstrate conformity to others;
  - seek certification/registration of its BCM Program by an accredited third party certification body; or
  - make a self-determination and self-declaration of conformity with this International Standard.

- Emphasis on setting the objectives, monitoring performance and metrics.
- Clear expectations on management.
- Careful planning for and preparing the resources needed for ensuring business continuity.
- Standard is made of ten “clauses”, seven of which are directly related to the proper development and maintenance of a BCM Program.
Clause 4 – Context of the organization (Scoping)

- Understanding the organization, both internal and external needs, and setting clear boundaries for the scope of the management system.
- Understand the requirements of relevant interested parties, such as regulators, customers and staff.
- Understand the applicable legal and regulatory requirements.

Clause 5 – Leadership

- Sets clear emphasis on the need for appropriate leadership of BCM relative to resource allocation and BCM policy.

Clause 6 – Planning

- This requires the organization to identify risks to the implementation of the management system and set clear objectives and criteria that can be used to measure its success.

Clause 7 – Support

- The day-to-day Program Management via competent resource(s) serving as staff with:
  - relevant (and demonstrable) training,
  - supporting services,
  - awareness, and
  - communication vehicles (both internal and external) focusing on format, content, and timing.

- Program supported by appropriately managed documented information policies and procedures governing creation, update and control of information.
Clause 8—Operations

- Risk Assessment
  - identification, analysis, and evaluation of risk.
- Business Impact Analysis
  - assessment and documentation of mission-critical processes inc. RTOs.
- Business Recovery Strategy
  - possible arrangements that will enable the organization to protect and recover critical activities.
- Business Continuity Procedures
  - flexible and straight-forward, and
  - includes Incident Response Structure and communications methodologies.
- Exercises, Testing, and Maintenance
  - processes of validating business continuity plans and procedures to align with selected strategies and capable of providing response and recovery results within agreed to timeframes.
Clause 9 – Evaluation

Requires that the organization select and measure itself against appropriate performance metrics. Reviews include:

- analyzing the extent to which the organization’s business continuity policy, objectives and targets are met;
- measuring the performance of the processes, procedures and functions that protect its prioritized activities;
- monitoring compliance with this standard and the business continuity objectives;
- monitoring historical evidence of deficient BCM Program performance;
- conducting internal audits at planned intervals; and
- evaluating all this in the management review at planned intervals.

Clause 10 – Improvement

Identifies requirements and actions to improve effectiveness and efficiency of the BCM Program over time and ensure that corrective actions. Using the results from the evaluation tools discussed in Clause 9 as primers for continuous improvement.
Evidence to Gather – Virtual &/or Physical

- Project Plans
- Program Charter & Governance Documentation (inc. Sr. Leadership support)
- BCM Methodology
  - Software
  - Internal
- Emergency Response Plans (site & threat specific) – Trained personnel & exercises
- Crisis Management & Crisis Communication Plans (inc. ENS) - Tested
- BIA Results – Current & Approved
  - IT/BIA Gap Analysis – inc. remediation if appropriate
- BCPs - Validated by BUs & maintained in a secure repository
- Exercise Documentation – Scenarios, participants, & After-Action Reporting
- Awareness Programs – e.g., Intranet, NEO, Post-Event Reporting
- Maintenance Program
Sample BCM Maturity Model

Continuing Growth, Improvement, & Maturity

<table>
<thead>
<tr>
<th>Level 1 Ad Hoc</th>
<th>Level 2 Early Formalization</th>
<th>Level 3 Established</th>
<th>Level 4 Embedded</th>
<th>Level 5 Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>No designated sponsor for the program</td>
<td>Cross-functional program steering committee exists but convenes infrequently</td>
<td>Program sponsorship and steering committee defined</td>
<td>BCM policies and standards documented</td>
<td>A culture of business resiliency exists and is part of day-to-day operations that includes regular communication to employees on plans and capabilities</td>
</tr>
<tr>
<td>No risk assessment / BIA performed</td>
<td>Risk assessment / BIA performed in some capacity</td>
<td>Risk assessment / BIA performed at least annually</td>
<td>Detailed business impacts and risks identified, quantified, and regularly reviewed</td>
<td>Importance of BCM to the organization is communicated to external parties</td>
</tr>
<tr>
<td>RTOs for systems and applications have not been identified</td>
<td>Functional RTOs defined, but not with full agreement of relevant business units.</td>
<td>List of system/application criticality and related RTOs in place for initial framework for recovery/restoration</td>
<td>Fully documented plans exist, including up-to-date contact information, recovery resource requirements, critical function listings, and identified dependencies (internal and external)</td>
<td>Vendor resiliency program in place</td>
</tr>
<tr>
<td>Business recovery strategies not documented</td>
<td>Limited consideration for business recovery needs vs. IT recovery capabilities</td>
<td>Understand critical dependencies</td>
<td>Detailed plans for failover and failback of all critical systems are developed</td>
<td>Robust testing performed throughout the year including tests with key vendors and ad-hoc/surprise tests</td>
</tr>
<tr>
<td>No maintenance, testing, training, or review procedures</td>
<td>Limited program testing has been performed</td>
<td>Some documentation exists for various BCM plan types:</td>
<td>Employees aware of program and involved in drills to successfully demonstrate recovery within stated RTOs</td>
<td>Changes to BCM program are automatically incorporated into BCM training materials</td>
</tr>
<tr>
<td></td>
<td>Limited maintenance procedures maybe in place</td>
<td>– ERP</td>
<td></td>
<td>System is in place to maintain employee competency for performing recovery responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– CMT</td>
<td></td>
<td>Senior management reviews the program at pre-determined intervals against defined metrics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– IT DR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– BCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Specific Contingency Plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Be sure to ask about acknowledged maturity or, if applicable, create one to show status of the Program.
Possible Use of Results

- Validate effort by BCM Team
  - Project Planning
  - Methodology
  - Documentation
  - Testing
  - Maintenance
- ID possible gaps in overall Program or specific component
- Budget analysis & refinement
  - People
  - Time
  - Funding
- Raise awareness
- Comply with outside inquiries
- Set Roadmap for future growth
Our disaster recovery plan goes something like this...

Someday we hope to have a budget.
Questions?