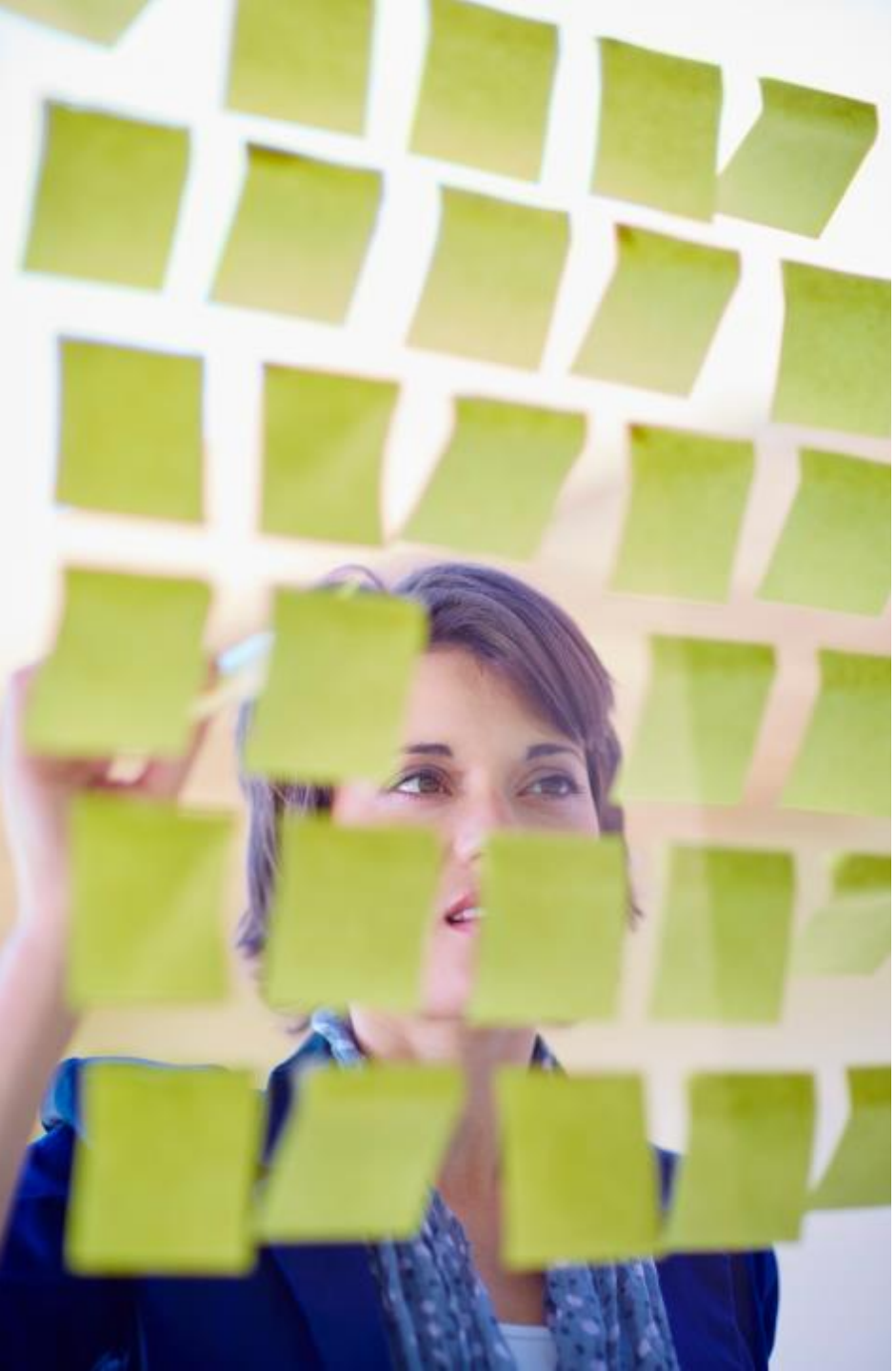
NASPL 2017
Professional Development
Seminar

Nashville, TN

Business Continuity Management
An Auditor's Perspective
July 25, 2017

Presented by
Mark Caiazzo, Principal

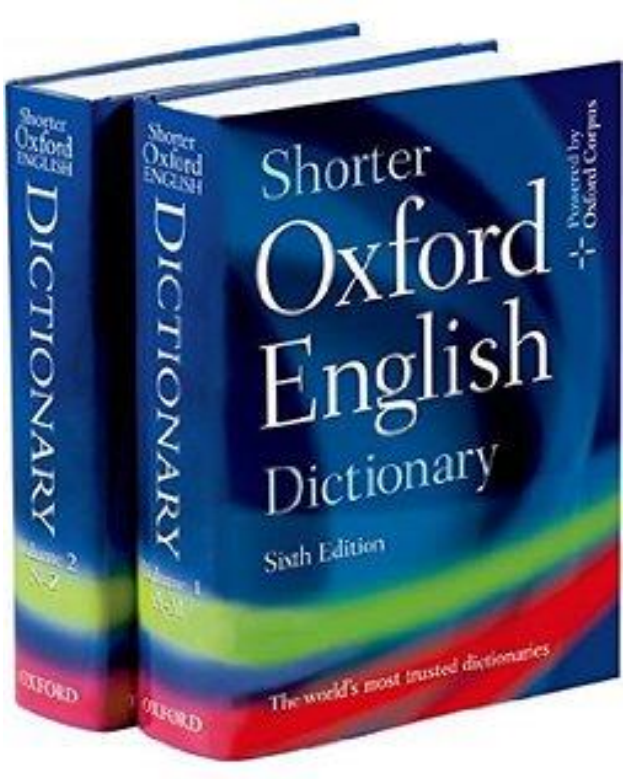
BerryDunn



Agenda

- Business Continuity Process
- BCM Evaluation
- Summary

The BCM Process

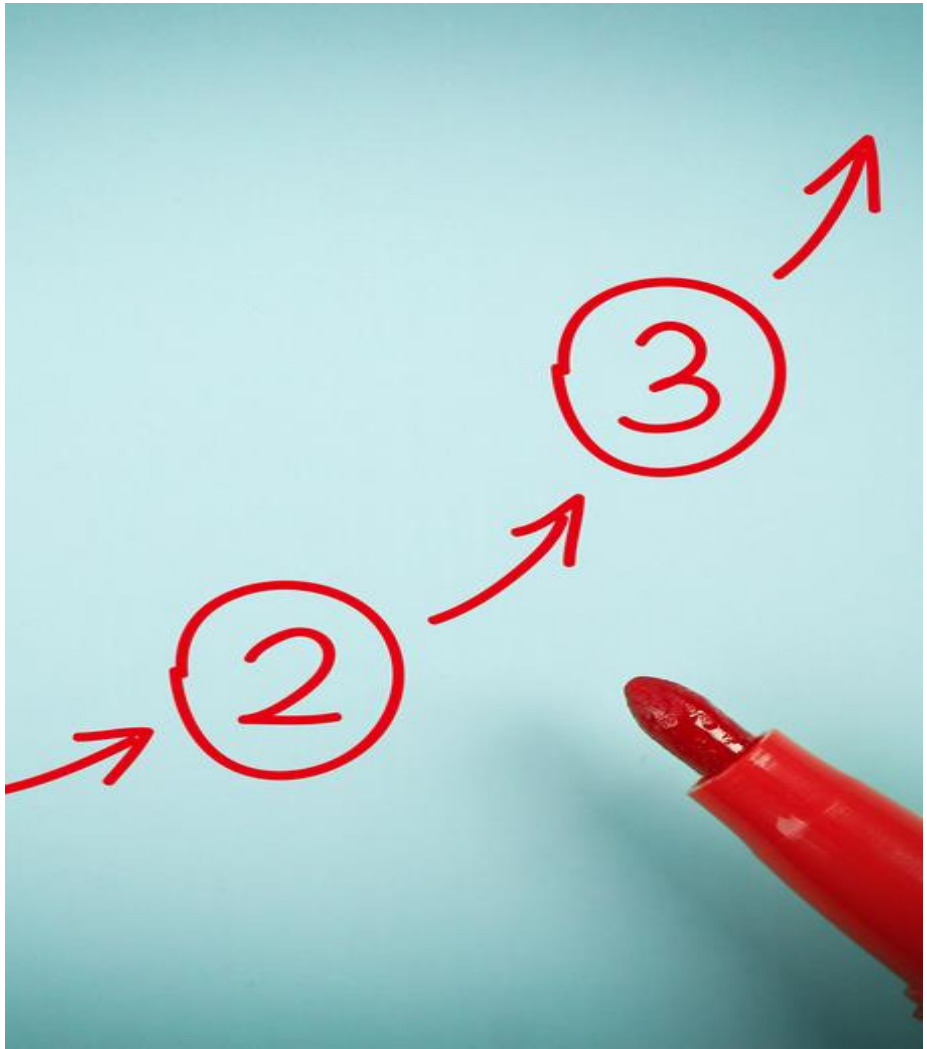


THEN …

"Business continuity management (BCM) is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities".

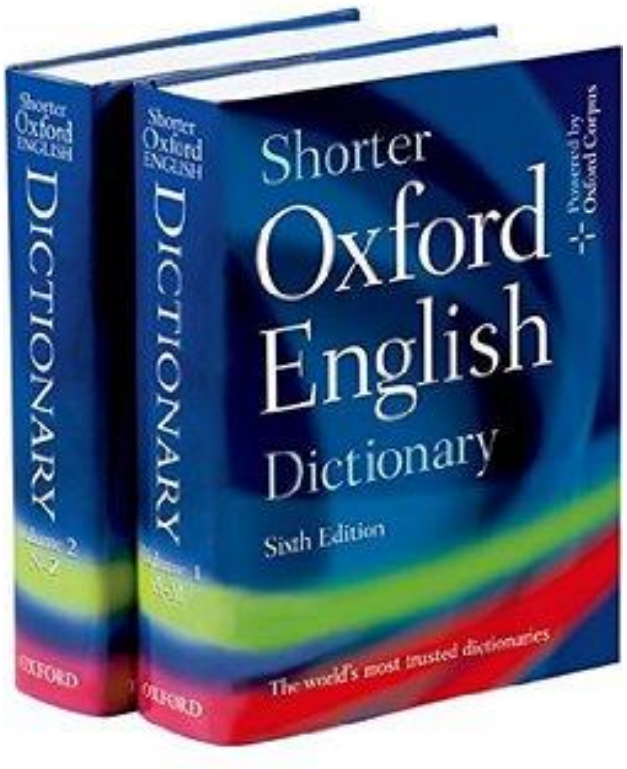
The Business Continuity Institute - 2001

Traditional Approach



- Assign responsibility
- Inventory IT systems, services, and resources
- Risk and impact analyses
- Develop and implement strategies
- Write the plan
- Train staff
- Test the plan to verify resources and tasks

The BCM Process



NOW ...

"Continuity 2.0 is a methodology for continuously improving an organization's response and recovery capabilities, with a focus on the continued delivery of services following an unexpected unavailability of people and/or resources".

Continuity 2.0 – A Manifesto - 2015

Continuity 2.0

- Culture
- Holistic approach
- Engage stakeholders from all levels of the organization
- Prepare for effect not cause
- Spend 80% of your time understanding, learning, and improving – 20% documenting
- Exercise for improvement, not to validate documentation
- Improve the way the plan document is used and delivered in an emergency
- Understand relevant performance benchmarks and how to monitor them

Definitions

- Business Continuity Plan or Continuity of Operations Plan (COOP) refers to the activities required to keep your operations running during a period of displacement or interruption of normal operation. Typically service focused, proactive

- Disaster recovery planning (DRP) refers to the activities of rebuilding your operation or infrastructure after the adverse event has passed. Typically IT focused, reactive, should be a part of overall BCM.

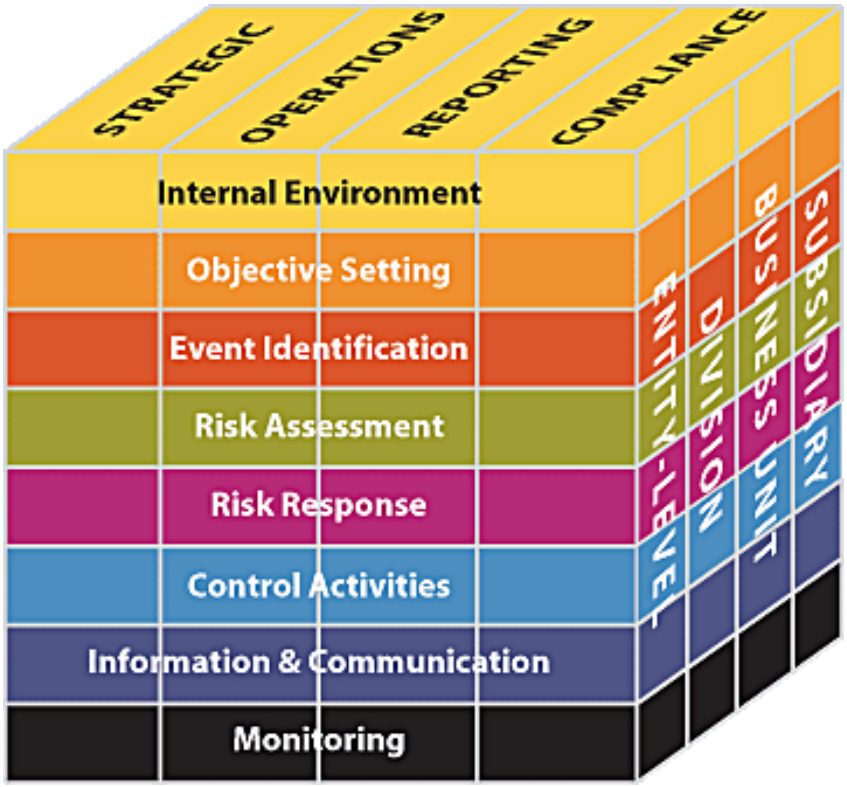
2. Audit Areas

- Initiation
- Risk and impact analyses
- Strategy development
- Planning
- Training
- Testing

Initiation (Governance)

- Sponsorship and support
- BCM budget (time, $)
- Program management process (PMI)
- Delegation of authority and succession
- Identification of relevant regulatory and governance issues
- Scope and goal setting
- Key performance indicators

Risk and Impact



COSO Cube

- Risk aware culture
- Updated inventory of essential services
- Recovery priorities and timescales
- Evolving risks
- Understand up and downstream risks
- Identification of relevant regulatory and governance issues
- Impact
- Efforts to build resiliency

Strategy Development

- Evidence of evaluation of options
- Consider people, places, and things – not just IT
- Binding arrangements – with built in transparency
- Strategies are tested
- Monitored for suitability on a periodic basis (vendor due diligence)

Processing Alternatives

- Reciprocal agreement
- Cold site
- Warm site
- Hot site
- Mobile unit
- Data vaulting

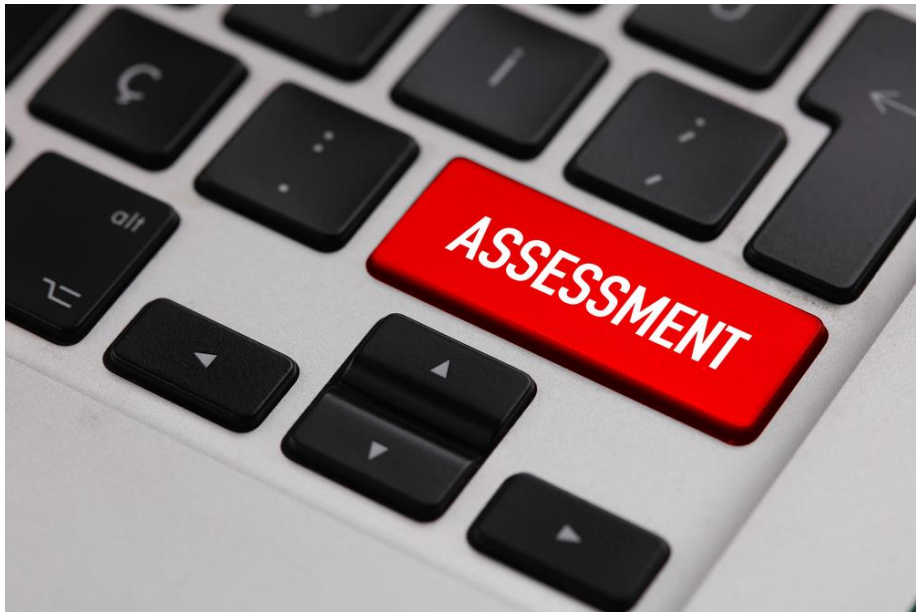
Planning

- Roles and responsibilities
- Communication plans (internal, external)
- Authority and actions for assessment, escalation, declaring a disaster, and activating the plan
- Identification of teams
- Maintain security and monitoring
- Documentation – keep it simple
- Plan maintenance and distribution

Training

- Response and recovery will require dedicated effort from people at every level of the organization
- Team members must have immediate and intuitive understanding of their roles
- Effective training requires appropriate and ongoing engagement at all levels of the organization

Testing



- Support the continuous improvement of response and recovery capabilities
- Testing at alternate location, with people, processes, and data running in “disaster mode”
- Test frequency depends on turnover of key personnel, number of business processes, and operational changes
- Involvement of persons with operational expertise
- Involvement of key subcontractors
- Post exercise review

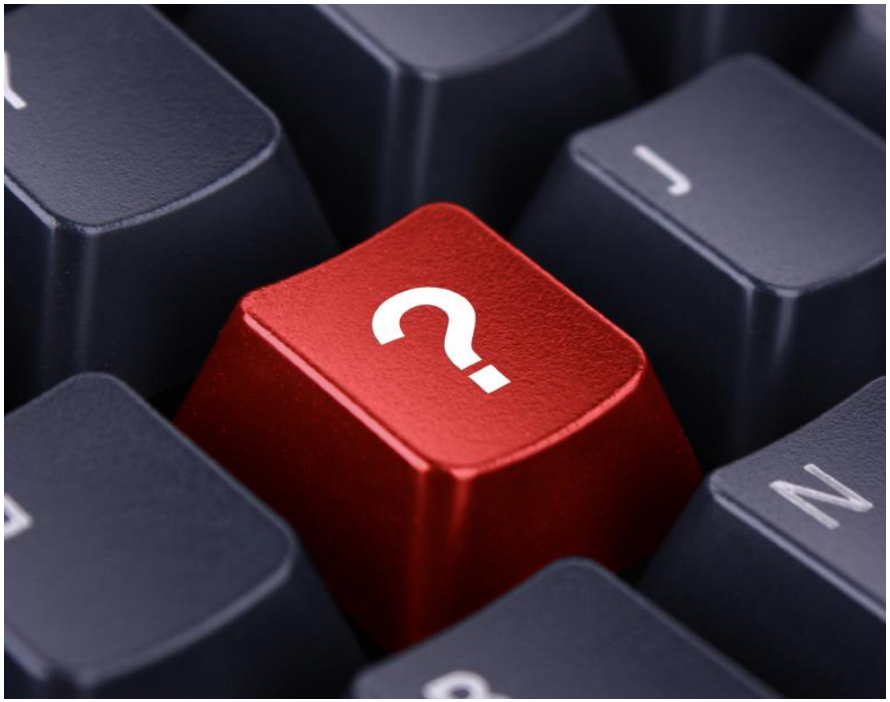
Test Strategies

- Checklist
- Walkthrough (tabletop)
- Simulation (dry run)
- Parallel (non-invasive)
- Full interruption (cutover)

Summary

- Evaluate the process, not the document
- Remember the 80-20 rule
- Understand the business objectives
- Talk with management, stakeholders, and BCM leadership
- Review meeting minutes, training documentation, test results
- Evaluate the plan
- Help improve the plan

Questions



Mark Caiazzo
mcaiazzo@berrydunn.com