Standards, Standards and more Standards...

Are you confused? And really which one should my organization follow?

Victoria EPICC Seminar
September 21, 2012
Presenter: Lisa Benini, MBCP
Agenda

- Definition
- Why Follow A Standard?
- What Standards exists today?
- How do they compare?
- How to apply these standards?
Definition

* Standard
  * A level of quality or attainment.
  * Something used as a measure for comparative evaluations.
  * A rule or set of rules or requirements which are widely agreed upon or imposed by government.

Guideline

- A non-specific rule or principle that provides direction to action or behaviour.
- A plan or explanation to guide one in setting standards or determining a course of action.

Why Follow A Standard?

- Due Diligence / Compliance
- Benchmark your Program
- Continuous Improvements
- Best Practices
- Audits
- Integration with other plans / programs
Why Follow A Standard? (cont’d)

- Identify and Analyze Loss Exposure
  - Preserve and protect life
  - Mitigate and minimize impact
  - Maintain Public Confidence Through Timely Information
  - Reduce Errors and Enable Recoverability
- Manage Stakeholder Expectations
- Monitor and Exercise the Program regularly
Why Follow A Standard? (cont’d)

- Communicate, Educate, Train
- Keep up to date
- Recognize Scarce Resources
- Ensure Appropriate Training and Capacity to carry out mandate
- Compare / Share Policies and Procedures
Why Follow A Standard? (cont’d)

* Designates Formal Structure
* Aligns with Strategic Objectives
* Command and Control Structure
* Address an All Hazard Approach
* Continuity / Recovery of Critical Ops
* Build the Infrastructure
* Protect Critical Infrastructure / Assets
Current Standards

* NPFA 1600: Version 2010 (US)
* BS 25999-1: 2006 British Standard (UK) - replaces PAS 56:2003
* AS/NZS 5050: 2010 Business Continuity (AUS/NZ)
* ANSI/ASIS/BSI BCM.01: Version 2010 (UK/US)
Current Standards

Current Standards

* ISO TC 223 – Societal Security:
  * ISO 22300 Vocabulary
  * ISO 22301 Continuity Management Systems – Reqmts
  * ISO 22311 Interoperability
  * ISO 22320 Emergency Management – Command /Control
  * ISO 22322 Public Warning
  * ISO 22323 Organizational Resilience – Reqmts / Guidance
  * ISO 22397 Public / Private Partnership
  * ISO 22398 Guidelines for exercises and testing
  * ISO 22399 Preparedness and Continuity Mgmt - Guidance
Current Guidelines

- The BCI Good Practice Guidelines 2008 / 2010 (UK)
- Professional Practices for Business Continuity Professionals - Disaster Recovery Institute International (DRII) (USA)
- Generally Accepted Business Continuity Practices - Disaster Recovery Journal (DRJ) (USA)
Most follow Plan-Do-Check-Act cycle
Most outline a management system
Some may be replaced by the new ISO 223## series
All have definitions
Not all definitions match
Vary in depth of detail
Some have process / lifecycle charts
Most recommend establishing a program
All recommend a policy, a coordinator, and program committee
What’s Different

* AS/NZS-5050: focus risks from disruptive events using AS/NZS ISO 31000:2009 risk mgmt principles, framework, and process
  * Adopted the ISO Guide 73:2009 Risk Mgmt Vocabulary
* BS 25999 has been replaced by ISO 223##
What’s Different

* CSA Z1600 and NFPA 1600 were very similar
  * Originally members on each Technical Committee
  * Lacking from business continuity content
* US adopted three of the standards: *PS-PREP*
  * ASIS SPC.1, BS 25999, NFPA 1600
  * Organizations finding hard to comply
Most guidelines don’t align to any particular standard
* Some are purely BCM and others are mixed of EM, RM, BCM and/or Security
## A comparison of ASIS/BSI BCM.01-2010 with ISO 22301 and PS-Prep Standards

<table>
<thead>
<tr>
<th>BCM Element</th>
<th>ISO 22301</th>
<th>ASIS/BSI BCM.01-2010</th>
<th>ASIS SPC.1:2009</th>
<th>BS 25999:2</th>
<th>NFPA 1600:2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Section 0.1</td>
<td>Section 0</td>
<td>Section 0</td>
<td>Introduction</td>
<td>Introduction</td>
</tr>
<tr>
<td>Plan-Do-Check-Act</td>
<td>Section 0.2</td>
<td>Section 0.2</td>
<td>Section 0</td>
<td>Introduction</td>
<td>Annex D</td>
</tr>
<tr>
<td>Scope</td>
<td>Section 1</td>
<td>Section 1</td>
<td>Section 1</td>
<td>Chapter 1.1</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>References</td>
<td>Section 2</td>
<td>Section 2</td>
<td>Section 2</td>
<td>Section 3.1</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>Terms &amp; Definitions</td>
<td>Section 3</td>
<td>Section 3</td>
<td>Section 3</td>
<td>Section 2</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>Business Continuity Management System</td>
<td>Section 4</td>
<td>Section 4</td>
<td>Section 4</td>
<td>Section 3</td>
<td>Annex D</td>
</tr>
<tr>
<td>Plan-Do-Check-Act</td>
<td>Section 0.2</td>
<td>Section 0.2</td>
<td>Section 0</td>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Section 5.3</td>
<td>Section 4.3</td>
<td>Section 4.2.1</td>
<td>Section 3.2.2</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>Planning</td>
<td>Section 6</td>
<td>Section 4.4</td>
<td>Section 4.3</td>
<td>Section 3</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Section 8.4.3</td>
<td>Section 4.4.1.2</td>
<td>Section 4.3.1</td>
<td>Section 4.1.2</td>
<td>Chapter 5.4</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>Section 8.4.3</td>
<td>Section 4.4.1.1</td>
<td>Section 4.3.1</td>
<td>Section 4.4.1</td>
<td>Chapter 5.5</td>
</tr>
<tr>
<td>BC Strategies</td>
<td>Section 8.4.4</td>
<td>Section 4.3</td>
<td>Section 4.2</td>
<td>Section 4</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>Implementation</td>
<td>Section 8.5</td>
<td>Section 4.5</td>
<td>Section 4.4</td>
<td>Section 4</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>Identifying Resources</td>
<td>Section 7.1</td>
<td>Section 4.5.1</td>
<td>Section 4.4.1</td>
<td>Section 4.3</td>
<td>Chapter 6.1</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>Section 6.4</td>
<td>Section 4.5.2</td>
<td>Section 4.4.1</td>
<td>Section 3.2.4</td>
<td>Chapter 6.6</td>
</tr>
<tr>
<td>BC Response</td>
<td>Section 8.5.4</td>
<td>Section 4.5.6</td>
<td>Section 4.4.7</td>
<td>Section 4.3.3</td>
<td>Chapter 6.9</td>
</tr>
<tr>
<td>Emergency Notification</td>
<td>Section 8.5.7</td>
<td>Section 4.5.7</td>
<td>Section 4.4.3</td>
<td>Section 4.3.2</td>
<td>Chapter 6.8</td>
</tr>
<tr>
<td>Business Continuity Plans</td>
<td>Section 8.4</td>
<td>Section 4.5.6.2</td>
<td>Section 4.3</td>
<td>Section 4.3.3</td>
<td>Chapter 6.7</td>
</tr>
<tr>
<td>Monitoring and Measurement</td>
<td>Section 9.1</td>
<td>Section 4.6.1</td>
<td>Section 4.5.1</td>
<td>Section 4</td>
<td>Chapter 7.1</td>
</tr>
<tr>
<td>Evaluation of Compliance</td>
<td>Section 8.7.2</td>
<td>Section 4.6.2</td>
<td>Section 4.5.2</td>
<td>Section 5.1</td>
<td>Chapter 7.1</td>
</tr>
<tr>
<td>Testing and Exercising</td>
<td>Section 8.6.1</td>
<td>Section 4.6.2.2</td>
<td>Section 4.5.2.2</td>
<td>Section 4</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>Records Management</td>
<td>Section 7.5</td>
<td>Section 4.6.4</td>
<td>Section 4.5.4</td>
<td>Section 3.4.2</td>
<td>Chapter 4.8</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>Section 7.3</td>
<td>Section 4.5.3</td>
<td>Section 4.4.2</td>
<td>Section 3.2.4</td>
<td>Chapter 6.11</td>
</tr>
<tr>
<td>Auditing</td>
<td>Section 9.2</td>
<td>Section 4.6.5</td>
<td>Section 4.5.5</td>
<td>Section 5.1</td>
<td>Chapter 8.1</td>
</tr>
<tr>
<td>Continuous Improvement</td>
<td>Section 10.2</td>
<td>Section 4.7.4</td>
<td>Section 4.6.5</td>
<td>Section 6.2</td>
<td>Chapter 8</td>
</tr>
</tbody>
</table>
How to apply these standards?
BCM Planning Lifecycle

 Understand Your Organization

 Performance Assessment

 Develop / Implement

 Planning

 Policy / Program Mgmt

 Management Review

 Embedding in the Organizational Culture

 2012-09-21
BCM Program Management

Plan
- Approve Policy
- Approve Standards & Practices
- Define Roles & Responsibilities
- Define Program Scope
- Agree Annual Goals

Do
- Maintain Framework
- Develop Action Plan
- Execute Planning Life Cycle
- Coordinate implementation
- Input to BCMS Audit

Check
- Track & Report Outcomes
- Aligned to changing Goals
- Aligned to leading practices
- Mitigates Risks
- Support BCMS Audit

Act
- Review & Amend Policy
- Amend Standards & Practices
- Amend Roles & Resp.
- Amend Scope & Goals
- Approve BCM Strategies
• Know your organization
  ✔ Scope defined to cover disruptions to facility, surrounding area or wide area.
  ✔ Established Framework / Governance
  ✔ Policy defined, documented, approved
  ✔ Leadership / Commitment
  ✔ Risk Assessment / Business Impact Analysis
  ✔ Program Management
    ✔ Mgmt Accountability (e.g. performance reviews)
    ✔ Program Committee
    ✔ Program Coordinator
Common Components

* Planning
  - Meet Legal /Regulatory Requirements
  - Completed Risk Assessment (monitor)
  - Completed Business Impact Analysis (refresh)
  - Strategy Development which covers
    - Prevention / Protection / Mitigation
    - Preparedness
    - Response / Continuity / Recovery
Common Components (cont’d)

- Development / Implementation
  - Organizational Structure
  - Roles, Responsibilities, Authority, Reporting
  - Training, Awareness
  - Competence (Position Descriptions)
  - Communications and Warnings
  - Incident Management
  - Finance and Administration
Common Components (cont’d)

- Development Implementation (cont’d)
  - Documentation / Document Control
  - Operational Procedures
  - Facilities for EOC, Alternate Worksites
  - Resources / Information Technology
  - Stakeholders
  - Interdependencies
Common Components (cont’d)

- Performance Assessment
  - Evaluations
  - Testing and Exercises
  - Corrective action
  - Maintenance
  - Monitoring and Review
  - Audits
- Management Review
  - Continuous Improvements
<table>
<thead>
<tr>
<th>Rating</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No process, no documentation.</td>
</tr>
<tr>
<td>1</td>
<td>Process exists and does not conform to the requirements of the standards, no documentation.</td>
</tr>
<tr>
<td>2</td>
<td>Process exists and partially conforms to the requirement of the standard, no documentation.</td>
</tr>
<tr>
<td>3</td>
<td>Process exists and conforms to the requirement of the standard but no documentation exists.</td>
</tr>
<tr>
<td>4</td>
<td>Process exists and conforms to the requirements of the standard, and documentation exists.</td>
</tr>
<tr>
<td>Clause</td>
<td>Requirement &amp; Review Questions</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Program Management</td>
</tr>
<tr>
<td>4.1</td>
<td>Leadership and Commitment</td>
</tr>
<tr>
<td>4.2</td>
<td>Program Coordinator</td>
</tr>
<tr>
<td>4.3</td>
<td>Advisory Committee</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Advisory Committee-established</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Advisory Committee-Input</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Advisory Committee-Members</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Has senior management provided leadership and assumed overall responsibility, accountability and authority for the program?
- Has the entity appointed a program coordinator authorized to keep current the program?
- Has an advisory committee been established?
- Does the advisory committee provide input to or assist the coordinator of the preparation, implementation?
- Does the advisory committee include the program coordinator and others who have the appropriate expertise, knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and applicable external representation?
Sample Compliance Matrix

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Complete, minor adjustments</td>
</tr>
<tr>
<td>Yellow</td>
<td>In progress, incomplete, needs improvement or minor risks/problems</td>
</tr>
<tr>
<td>Red</td>
<td>Not started, early stages of planning or major risks/problems</td>
</tr>
</tbody>
</table>
The CSA Z1600 Standard for Emergency Management and Business Continuity Programs was applied to how this organization has established its programs.

4 Program management

4.1* Leadership and commitment
Senior management shall provide leadership and assume overall responsibility, accountability, and authority for the program.

4.2* Program coordinator
The program coordinator shall be appointed by the entity and authorized to administer the program and keep it current.

4.3 Advisory committee

4.3.1*
An advisory committee shall be established as required by the entity’s policy.

4.3.2
The advisory committee shall provide input to or assist in coordinating the preparation, implementation, evaluation, maintenance, and revision of the program.

4.3.3*
The advisory committee shall include the program coordinator and others who have the appropriate expertise, knowledge of the entity, and the capability to identify resources from all key functional areas within the entity. Applicable external representation shall also be included.

4.4 Program administration

4.4.1 General
The entity shall have a documented program that includes the components described in Clauses 4.4.2 to 4.4.7.

4.4.2 Policy
The entity shall establish a policy that includes a vision, mission statement, roles and responsibilities, and enabling authority. The policy should be approved by the executive of the entity.

4.4.3* Program goals and objectives
The entity shall establish program goals and objectives.

4.4.4* Program plan and procedures
The entity shall establish program plans and procedures for the functions of prevention and mitigation, preparedness, response, and recovery.

4.4.5 Program budget
The entity shall establish a program budget and schedule that includes milestones.

4.4.6* Records management
The entity shall
* Critical people are available to support critical activities
* Corporate operational continuity is implemented
* Alternate facilities are pre-designated
* Minimum resource requirements for continuity is identified and secured
Key interdependencies are identified and agreements/arrangements are established and rehearsed;

Corporate computer systems are identified, prioritized, tested and available

Corporate telephony is accessible

The plans are maintained on a regular basis and exercised to familiarize the critical people how to use them and make sure they work.
Title Change: 
Emergency and Continuity Management Program

Structure and content changes:

* Preface 1 Scope, Purpose and Application
  2 Reference publications 3 * Definitions
  4 Program management 5 Planning 6 * Implementation
  7 Program evaluation 8 Management review

* Aligned more closely with ISO 22301
* Plan design – individual or integrated in any combo
* Use the EM framework from Public Safety Canada
  * Prevention/Mitigation, Preparedness, Response & Recovery
* Restructure Planning section (5)
Re-structure Implementation section (6):
- Prevention and Mitigation
- Preparedness
  - Response, Incident Management System, Response Plan
  - Communications and Warning
  - Continuity
  - Resource Management
  - Mutual Aid / Mutual Assistance
  - Facilities
  - Training
- Response
- Recovery
CSA Z1600 Public Review

- Enhanced Program Evaluation (7)
  - Evaluation
  - Exercises and Tests
  - Audit and Review
  - Corrective Action
- Enhanced Management Review (8)
  - Management Review
  - Continuous Improvement
CSA Z1600 Public Review

* Closing date to submit comments on the draft is October 1st, 2012

* Link to the CSA Public Review Website
  * [http://publicreview.csa.ca](http://publicreview.csa.ca)

  The draft is under the link titled “Occupational Health & Safety”
Does my organization have a mature BCM program in place?

Does my organization have to align to a certain standard due to the industry, sector or jurisdiction?

To what level of detail is my organization’s BCM Program required to benchmark with?

What am I trying to achieve from using a standard?
Resources

CSA Z1600: 2008
http://www.csa.ca/cm/ca/en/z1600-emergency-management

NFPA 1600: 2010
http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1600

BSI 25999: 2006

AS/NZS 5050: 2010

ANSI/ASIS/BSI BCM.01: 201
Resources

ASIS SPC 1: 2009
http://www.asisonline.org/guidelines/or.xml

ISO 22399: 2007

BCI Good Practice Guidelines
http://www.thebci.org/gpg.htm

Professional Practices (DRII)
https://www.drii.org/professionalprac/index.php

Generally Accepted Practices (DRJ)
http://www.drj.com/resources/resources/generally-accepted-practices.html
"The unfortunate truth is our ability to imagine and plan for catastrophic disasters is woefully inadequate."\(^1\)

A broad assessment from Dr. Irwin E. Redlener, the director of the National Center for Disaster Preparedness\(^{TM}\) at Columbia University\(^{®}\)

\(^1\) Business Week\(^{®}\), 9/19/05, p. 35
Thank you.

Lisa Benini, MBCP
Benini Consulting Ltd.
Ltbenini@gmail.com
+1 250.813.2435
www.beniniconsulting.com