Agenda

• Governance: Definition and Qualities
• Benefits of a Governance Document
• How Standards Fit into the Picture
• The Governance Document Itself
• Next Steps
Governance: Definition and Qualities
Governance

• In its simplest form, governance is about authority, decision-making, and accountability.
  – Within an organization, the term ‘governance’ determines who has authority, who makes the decisions, and how the organization is kept accountable.

• Good governance is about the processes for making and implementing decisions.
  – It’s not about making ‘correct’ decisions, but about the best possible process for making those decisions.
Governance
Good Governance Qualities

• Good governance is:
  – Accountable.
  – Transparent.
  – Responsive.
  – Equitable and inclusive.
  – Effective and efficient.
  – Participatory.

• Lastly, it follows the rule of law.
Benefits of a Governance Document
Governance Brings it all Together

Enterprise Risk Management

Business Continuity Program Governance

Incident Management

Emergency Response  Business Continuity  Disaster Recovery  Crisis Communications
Benefits of a Governance Document

• There are three primary benefits to investing the time and energy in creating a Business Continuity (BC) Governance Document:
  – *Create an internal commitment.* To overcome the inertia that often prevents ‘overhead’ programs from developing.
  – *Define the end-state.* To establish the size, scope, and structure of the BC program.
  – *Define the mechanisms for maintaining the program over time.* To ensure that the capability, once built, remains viable.
How Standards Fit into the Picture
Governance and Standards

• How standards fit into the governance picture:
  – First, you need an authoritative guide to build a program, one that is credible and widely recognized.
  – Standards are business tools that help to ensure quality, standardization, conformity, and assessment activities. They can lead to a competitive advantage by increasing efficiencies, minimizing errors, and reducing recovery time.

• This presentation will focus on two standards:
  – ISO 22301.
  – NFPA 1600.

• These two were chosen because:
  – They are both widely used in North America (and, in the case of ISO 22301, much of the rest of the world).
  – They represent two distinct perspectives.
  – At the end of the day, they both address the same fundamental requirements.
Two Standards

• Both ISO 22301 and NFPA 1600 require:
  – Various program management and control functions.
  – Planning and assessment functions (in the form of a Business Impact Analysis and a Risk Assessment).
  – Core operational functions:
    o Incident Management (aka Crisis Management).
    o Business Continuity (Business Process Recovery).
    o Technology Disaster Recovery.
    o Emergency Response.
    o Crisis Communications.
Two Standards

• ISO 22301 and NFPA 1600 take different approaches to the same problem.
  
• ISO 22301:
  – Geared to an international audience.
  – Structurally consistent with other ISO standards, including use of the “PDCA” paradigm.
  – Perspective is overall preparedness, self-described as “generic.”

• NFPA 1600:
  – Consistent with other standards developed by NFPA.
  – More prescriptive with some requirements.
  – Slightly more emphasis on disaster prevention and incident management.
Two Standards

- Either standard will work in terms of defining a comprehensive and robust business continuity program.
- As noted, both define the basic elements of a program in fundamentally equivalent terms.
- Therefore, a preference for one over the other will be largely based on factors other than core content.
Golden Rule of Standards Compliance

- Absolute conformity to a standard does NOT always translate into an effective functional capability.

- Compliance certifications are NOT a substitute for rigorous exercises and critical program reviews.
Leveraging a Standard

• Picking a standard to use is the easy part. The next step is to determine how to effectively leverage the standard to move your program forward.

• Two general approaches:
  – Option One: Brute force.
  – Option Two: “Standards are a guide”

• Brute force approach:
  – Lobby to have your company adopt a policy mandating fully compliance to a standard.
  – Insist on strict compliance, no matter what.
  – Use the standard as a bludgeon to force cooperation and gain budget.
  – *We don’t recommend bludgeoning your colleagues.*

• We recommend taking the “standards are a guide” approach.
Leveraging a Standard

• Core idea on using the “standards are a guide approach” is to build your foundation in a Program Governance model.
• In general, a policy mandate is too narrow. It boxes you in to a “do or die” approach.
• The better alternative is to create a more flexible mandate, using a Program Governance framework as the implementation tool.
  – Lobby to have your company adopt a policy that requires an “effective business continuity capability.”
  – Be prepared to compromise on certain requirements when doing so is in the best interest of the company.
  – Work with your internal and external auditors to establish pragmatic criteria for measuring compliance.
The Governance Document Itself
The Document Itself

• It may be clear now that the Governance Document may serve multiple purposes:
  – Promote executive management understanding and support of the program, and codify that support in the form of a sensible business continuity policy.
  – Define the role that a business continuity standard will play in defining the program.
  – Create a sense of budget certainty in the form of requirements for program exercises and reviews.
• Let’s take a look at what the Governance Document should contain.
Governance Document

- EMSS likes to divide the Governance Document into two major sections:
  - Administration and Planning.
  - Operational.
- Each section contains elements keyed to the business continuity standard that’s been selected.
- We’ll address the major components of each section in turn.
Administration and Planning

• This section typically contains three major elements:
  – 1. Program Management and Structure:
    o Policy.
    o Scope and Goals.
    o Operational Structure.
    o Resources.
    o Roles, Responsibilities, and Delegated Authorities.
    o Legal and Regulatory Requirements.

Continued…
Administration and Planning

• This section typically contains three major elements (cont’d):
  – 2. Program Oversight and Validation:
    o Monitoring and Measuring.
    o Management Review.
    o Continuous Improvements.
    o Exercises and Training.
  – 3. Program Planning:
    • Risk Assessment.
    • Business Impact Analysis.
    • Business Process Recovery Strategies.
Developing the Admin and Planning Section

• Hold a whiteboard session with the “right people.”
• Prepare some sections as a “straw man.” Leave other sections framed as “general discussion.”
• Get the “right people” into a room for a discussion. It should last between 90 minutes and 2 hours.
  – Introduce the areas, discuss, debate, and come to an agreement
• This fosters commitment, a deeper understanding of the program, buy-in, and support.
Sample Policy Phrases

• “The Company is committed to creating and maintaining a viable Business Continuity Program that addresses the protection and preservation of people, mission, and assets.”

• “The Company’s Business Continuity Program will be developed and maintained in manner that is appropriately scaled to the size and mission of the organization, and that emphasizes simplicity to the maximum degree possible without sacrificing operational capability.”

• “All managers and employees are expected to be fully aware of the Program and to participate in Program-related activities as directed.”
Sample Scope and Goals

• “The scope of the Program includes all business activities associated with all Company facilities.”

• “The goals of the Program are to:
  – Ensure the safety and well-being of Company employees.
  – Protect Company’s ability to execute and fulfill its operational mission.
  – Protect Company’s physical assets.
  – Ensure Company’s ability to communicate quickly and effectively to all stakeholders.
  – Strike an appropriate balance between potential losses and Program costs.”
Program Operational Structure Discussion

Review and discuss the following Program model:

Enterprise Risk Management

Business Continuity Program Governance

Incident Management

Emergency Response  Business Continuity  Disaster Recovery  Crisis Communications
Sample Program Roles and Responsibilities

• “Executive Management: General Program oversight, appoints Steering Committee and Program Sponsor.”
• “Steering Committee: Review Program status and direction, allocate resources, appoint Program Sponsor.”
• “Program Sponsor: Provide senior leadership and management over all Program activities, appoint Program Manager.”
• “Program Manager: Provide “hands on” program/project management over all Program activities.”
# Sample Program Role Authorities

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Management Team</td>
<td>Steering Committee</td>
<td>Oversee the Business Continuity Program and provide guidance and direction to the Program Sponsor. Allocate resources necessary to achieve core Program goals and objectives.</td>
</tr>
<tr>
<td>Executive Management Team</td>
<td>Program Sponsor</td>
<td>Prioritize Program development and validation activities and distribute available resources to accomplish identified Program goals.</td>
</tr>
<tr>
<td>Program Sponsor</td>
<td>Program Manager</td>
<td>Organize and direct Program development and validation activities. Create and publish multi-year Program activity calendar.</td>
</tr>
<tr>
<td>Executive Management Team</td>
<td>Incident Management Team (IMT)</td>
<td>Prioritize response and recovery tasks and direct the allocation of all company response and recovery resources when the IMT is activated.</td>
</tr>
</tbody>
</table>
Program Review and Validation Discussion

• Discuss how you believe the following requirements should be addressed:
  – **Management Reviews**: Which management team(s) should review the status of the Program? At what frequency?
  – **Monitor and Measure**: Who should establish Program metrics? Who should review the results?
  – **Exercises and Training**: What should be exercised? How often? Who reviews the results? Who should be trained? How often? Who reviews the results?
  – **Continuous Improvement**: Who should identify opportunities for Program improvement? How will those improvements be approved for implementation?
Program Planning Discussion

• Discuss how you believe the following requirements should be addressed:
  – **Risk Assessment:** How often should your Risk Assessment results be updated? Which management team(s) should review the results?
  – **Business Impact Analysis:** How often should your BIA results be updated? Which management team(s) should review the results?
  – **Business Unit Recovery Strategies:** How often should departmental recovery strategies be reviewed? Which management team(s) should validate the results?
Operational

• This section typically contains the following operational elements:
  – Incident Management.
  – Crisis Communications.
  – Business Continuity.
  – Technology Disaster Recovery.
  – Emergency Response.

• Each section contains:
  – Overview.
  – Brief description of the plan.
  – Responsibilities and authorities.

• Many companies also include pandemic response as a distinct operational element – a practice we highly encourage!
Next Steps

• Now what?
  – Secure an executive sponsor.
  – Select a steering committee; get your sponsor to approve and endorse the members.
  – Bring the steering committee together to “whiteboard” the major sections of the document.
  – Develop, review, refine, repeat.
  – It is an iterative process and will improve over time.
KEEP CALM AND GET GOING
Thank you

Regina Phelps
Emergency Management & Safety Solutions
San Francisco, California
@ReginaPhelps
Linkedin.com/in/reginaphelps
Regina@ems-solutionsinc.com
www.ems-solutionsinc.com