

Business Continuity Trends, Requirements and Expectations in 2009

Brian Zawada (MBCP)
Director of Consulting Services
Avalution Consulting

Overview



- What Is Business Continuity?
- The Value Proposition
- What's Changed?
- Management Expectations
- Leading Practices
- The Role of the Internal Auditor
- Discussion





“Once a standard takes hold,
people start to focus on the quality
of what they do as opposed to how
they are doing it.”

Thomas L. Friedman

The World Is Flat – A Brief History of the 21st Century



What Is Business Continuity?

A risk management program that focuses on designing, implementing and maintaining strategies that not only minimize the likelihood of a disruptive event, as well as strategies that ensure an efficient response to a disruptive event and thus the availability of business processes and technology assets in accordance with management-approved objectives.

What Is Business Continuity?



Prevent disruptions - but if you can't, minimize downtime and business impact.

What Is It (Really)?



Crisis Management

Strategies and actions designed to protect people, property and business functionality, while preparing for recovery of critical processes.

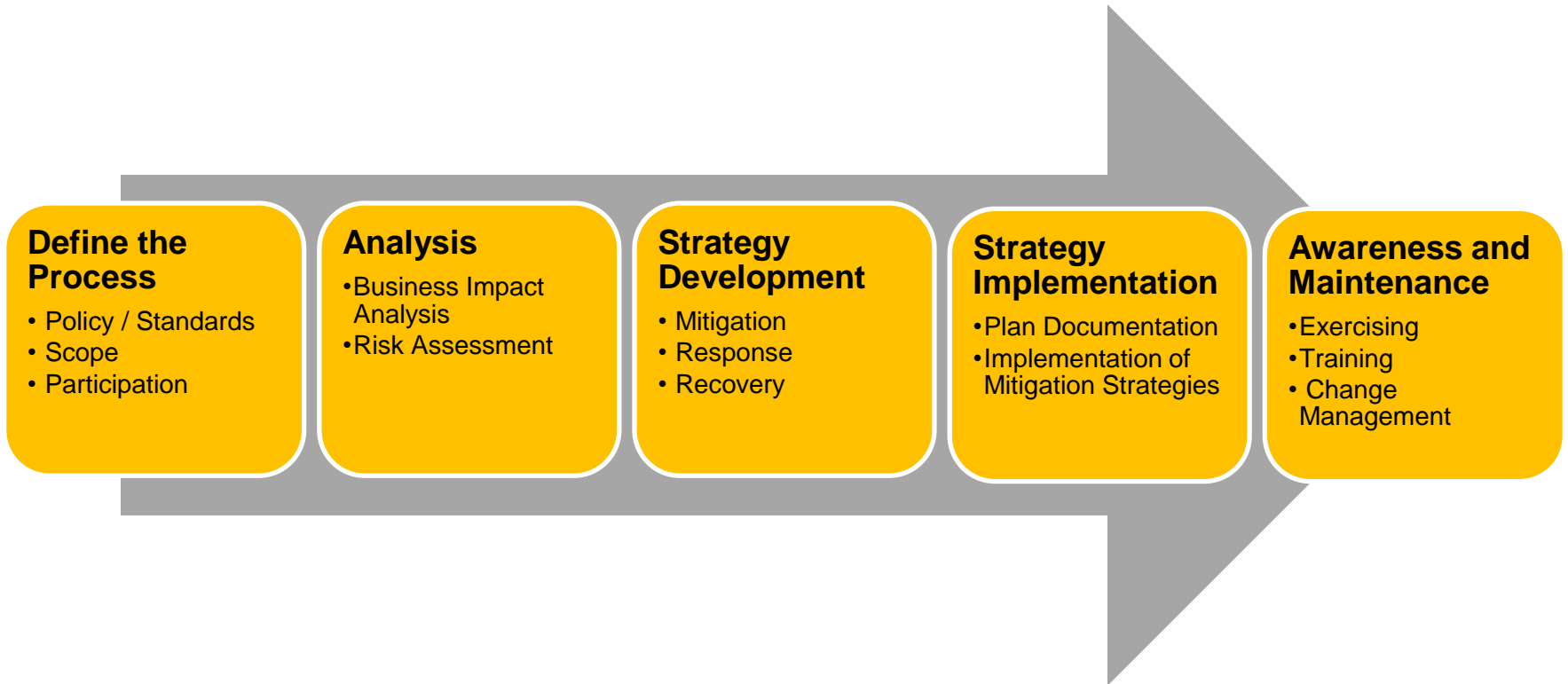
Business Recovery

Resuming critical business processes in a reasonable timeframe and to a minimum acceptable level using alternate facilities, resources, personnel, technologies and/or processes.

IT Disaster Recovery

Resuming critical technologies (applications, communications and PCs/printers) based on business requirements.

Methodology





The Relationship to ERM

- ERM Is The Umbrella Program
 - Business Continuity Is Just One Component
 - Balance Between Proactive and Reactive
- Your Business Continuity Professional Is Learning About ERM and Enterprise Risk Assessment Concepts
 - If Not, Educate Them!
 - No More Rank Ordering Threats

Why Is Business Continuity Important?

- Help the organization respond to an event appropriately, using predetermined strategies
- Identify response and recovery strategy details
- Provide “checklists” of steps to take
- Define methods to communicate with key stakeholders



But the plan isn't as important as the planning process...



Your Executive's Motivator(s)

- Fear
 - Financial Loss
 - Market Share Loss
 - Reputational Impairment
- Increased Customer Confidence
- Governance Expectation
- “The Right Thing To Do”



Management Expectations



- Reputation Protection
- Meet Stakeholder Expectations
- Standard of Care
- Keep the “Bad Stuff” From Occurring



Leading Practices



- Management System Concepts
- Strong Governance Controls
- Decentralized Program Execution
- Six Sigma Based Analytic Processes
- The Extended Enterprise
- Training and Awareness
- The Use of Software
- Scorecards



What's Changed?



- Not Just IT
- Not Just Internal
- Getting Credit
- New / Changing Standards
 - BS 25999
 - NFPA 1600
- Convergence
- Proactive and Reactive
- Certification



Certification Landscape



- ☑ BS 25999
- ☑ ISO 27001
- ☑ EMAP
- ✘ ISO 22399
- ✘ ISO 24762
- ✘ NFPA 1600
- ✘ Title IX





What is BS 25999?

- Authored by the British Standards Institute
- Two Part Document
 - Part I: Code of Practice (published in November 2006)
 - Part II: Specification (published in November 2007)
- Designed As An International, “Umbrella” Standard with Certification in Mind
- <http://www.bsimamerica.com>



Not Just a European Standard



What is Title IX?

- Public Law 110-53 (signed into law 8/3/2007)
- Title IX – Voluntary Certification Program
 - Develop guidance or recommendations; identify best practices
 - Develop and promote a program to certify the preparedness of private sector entities that voluntarily choose to seek certification
 - Provide business justification for preparedness and adoption of voluntary preparedness standards

The Certification Value Proposition



Strength of Criteria	Criteria Influencing The Certification Decision-Making Process
<input type="checkbox"/> (Strong)	Customer Demand
<input type="checkbox"/> (Strong)	Differentiate in the Marketplace
<input type="checkbox"/> (Moderate)	Cost Savings Opportunities
<input type="checkbox"/> (Moderate)	Senior Leadership Inquiries
<input type="checkbox"/> (Moderate)	Maintaining Focus
<input type="checkbox"/> (Weak)	Integration
<input type="checkbox"/> (Weak)	Life-cycle Concept

Building Trust and Confidence

The Role of the Internal Auditor



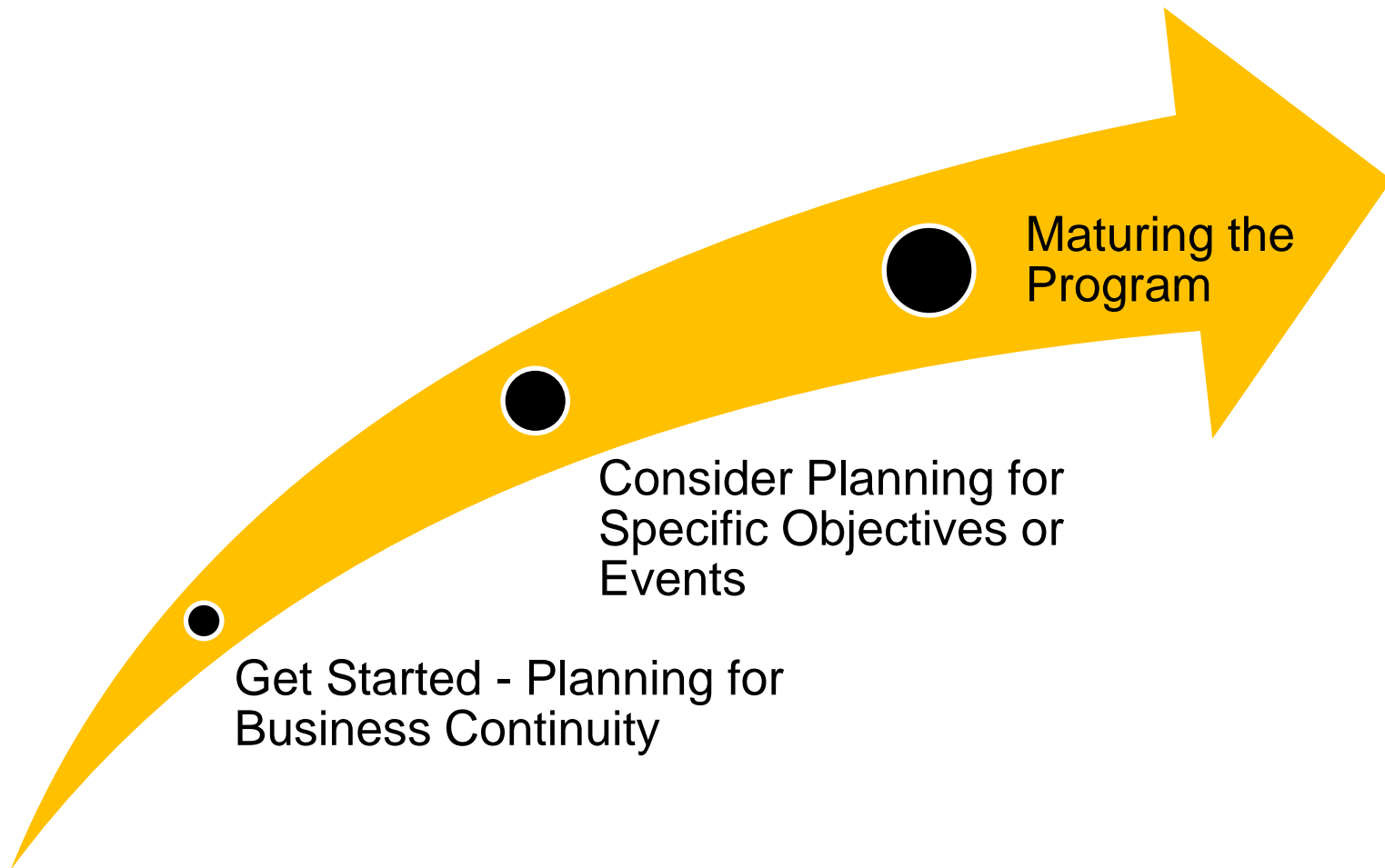
1. Business Case Communication
2. Catalyst for Change
3. Sharing Risk Metrics
4. Measure Performance
5. Translate

The Role of the Internal Auditor – Business Case Communication



- Assist Management with Understanding Business Continuity Risk
 - Ad Hoc Responses Won't Work Well

The Role of the Internal Auditor – Catalyst for Change



The Role of the Internal Auditor – Sharing Risk Metrics



- Share Risk Metrics with Your Business Continuity Team
 - Promote Alignment
 - Use of a Common Risk Tolerance Measurement

Analysis As A Driver



- Many Organizations *Just* Use a BIA to Figure Out Recovery Objectives and Ignore the Risk Assessment Completely
- A Strong BIA and Risk Assessment Should Articulate the Need for Business Continuity Throughout the Organization
 - Identifies the “Risk” That Business Continuity Will Mitigate
 - Drives Scoping Decisions
 - Sets the Table for Strategy Discussions

The Role of the Internal Auditor – Measure Performance



- Measure Business Continuity Performance;
Enable Focus and Repeatability
 - Process-based measurement, not plan reviews

The Role of the Internal Auditor – Translate



- Help Overcome Resistance
 - Value Proposition



Root Causes

- The Business Continuity Team Lacks an Understanding of:
 - What's Strategically Important to the Organization
 - How the Organization and its Executive Managers Measure Performance
 - Management Risk Tolerance
- A Focus on Reacting to Crisis Events, Not Preventing Them
- Terminology That No One Understands
- Failing to Explain the Importance and Value Offered by Business Continuity

The Business Continuity Value Proposition



- Understanding what threats are most likely to severely impact operations
- Mitigating the likelihood that high risk threats will impact operations, potentially causing an interruption to customer-facing services
- Developing process documentation to efficiently enable the resumption of critical work streams during an incident
- Ensuring continuity of operations through facilities, supply chain, information and communications readiness
- Creating a leave-behind roadmap for next level leadership should primary leadership become unavailable
- Highlighting personnel and knowledge deficiencies for remediation (succession planning, cross training and intellectual capital)

Conclusions and Discussion



- Higher Expectations
- Maturation of Business Continuity Thinking
- New Standards and Methods to Measure and Prove Readiness
- Internal Audit As a Process to Ensure The Organization:
 - Gets Started
 - Addresses the Correct Activities
 - Maintains a Repeatable Program



Contact Information



Brian Zawada

- Director of Consulting Services
- brian.zawada@avalution.com
- www.avalution.com
- 800.941.0381 (o)
- 330.321.8650 (m)
- 216.803.6738 (f)

Presentation Abstract



The business continuity profession is undergoing radical change. Organizational certification, demanding customer expectations and new standards are all contributing to enhanced readiness – but also organizational challenges. This presentation will summarize business continuity trends and how the internal audit professional can support its internal business continuity experts in meeting emerging requirements and expectations.