

***What do we need to know...
to achieve an Effective...***

“Business Impact Analysis Process”

Lillibett Machado-Principal Consultant
MBA, CISM, CISA, CGEIT, CBCP, ITIL-BSM

Business Impact Analysis (BIA)

“A BIA will...

...identify the impacts resulting from business interruptions

What should we know?

How do we get this information?

...provide techniques that can be used to quantify and qualify such impacts

How do we quantify and qualify such impacts?

What techniques should we use?

...identify time-critical functions, their recovery priorities, and interdependencies so that recovery time objectives can be established and approved

Business Impact Analysis Governance Concerns

- Lack of a Framework or Policy
- Lack of formal BIA Procedures
- Lack of acceptance as a Process
- Lack Organizational Responsibility

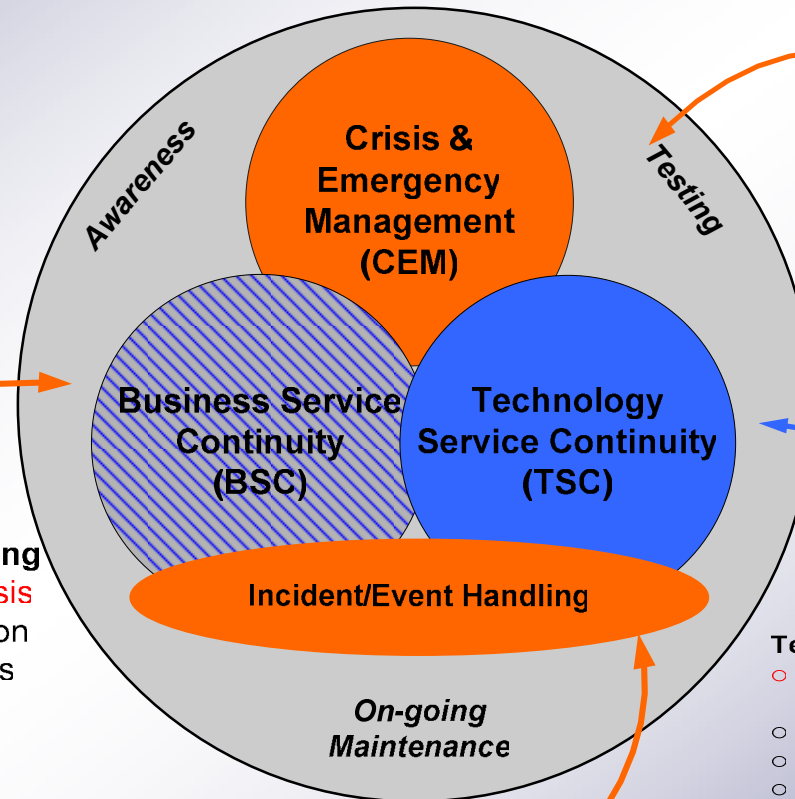
Comprehensive Business Continuity Management (BCM) Framework

Enterprise-Wide Approach

- Business Process Focused
- Operational Risk Mitigation
- Business Impact Analysis
- Resilience & Continuity Solutions
- Regulatory & Standards Integration

Business Service Planning

- Business Impact Analysis
- Incident/Event Escalation
- Resource Requirements
- Business Resumption Strategies
- Testing & Awareness



Crisis and Emergency Management

- Emergency Planning & Response
- Command Center Operations
- Communication Coordination
- Logistics Support
- Incident/Event Management

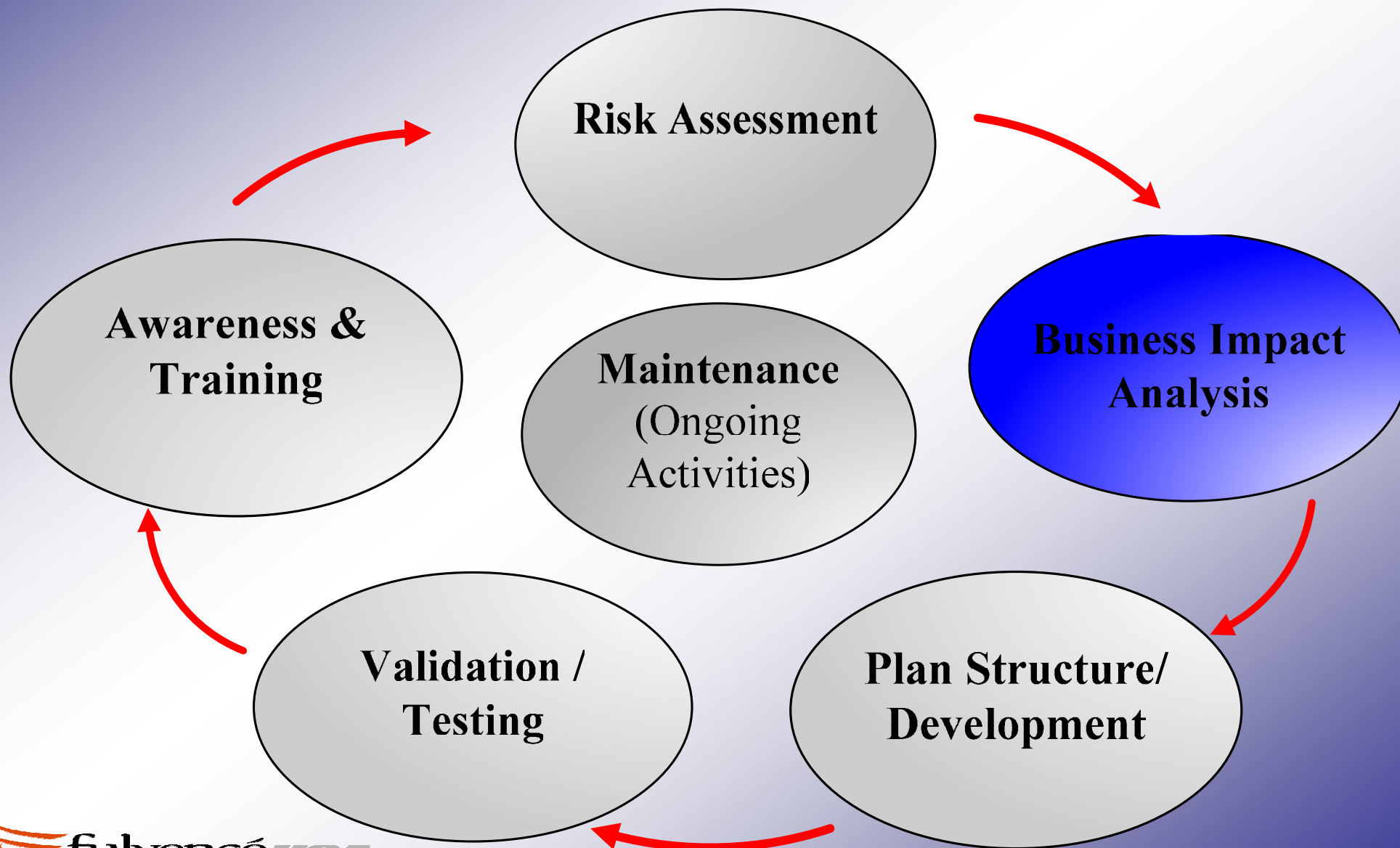
Technology Service Planning

- Technology Service Impact Analysis
- Incident/Event Escalation
- Recovery Strategies
- Resource Requirements
- Testing & Awareness

Availability provides

- Continuous Operations
- Disaster Avoidance
- Preventive Capabilities
- Optimal Controls & Risk Mitigation

Business Continuity Process



Business Impact Analysis Process

Planning:

- Define/develop questionnaires, surveys or templates

Identifying the Key Business Processes:

- Identify Business Functions
- Identify Key Processes
- Develop process Workflows
- Identify process Impacts and Potential Risks (i.e. Financial Loss)
- Established “Process Risk Level”
- Define process Recovery Time Objective (RTO)
- Determine process External Dependencies
- Determine process Work Schedule & Peak Times
- Determine process Key Resources

Identifying Key Business Process Components:

- Determine process Components and Impact
- Identify Data Components & “Recovery Point Objectives”

BIA Reporting: Ex. All Processes and Components - By Business Unit

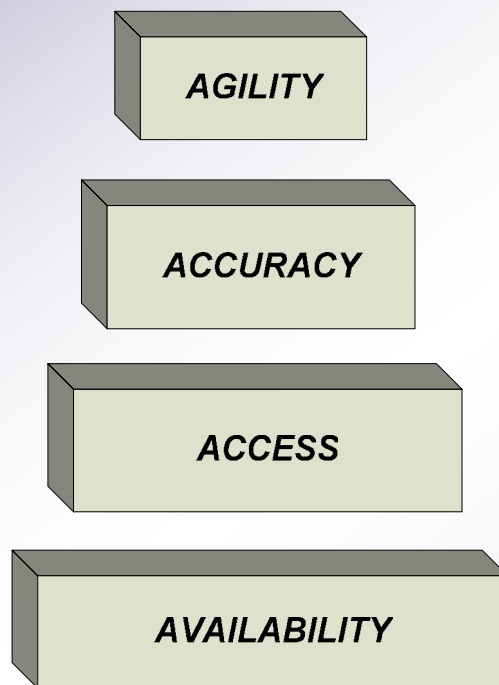
<u>Component Name</u>	<u>Component Type</u>	<u>PI</u>	<u>RTO</u>	<u>CI</u>	<u>RPO</u>
BU: Business Process:	<u>Electronic Funds Transfer: Wire Processing</u>				
Network Provider	Service Provider	5	< 04 Hours	4	(not applicable)
Money Transfer System	Application - Software	5	< 04 Hours	4	(not applicable)
Tel Com Access	Application - Software	5	< 04 Hours	3	(not applicable)
JHA Silverlake	Application - Software	5	< 04 Hours	4	(not applicable)
ABC Net	Application - Software Emulation	5	< 04 Hours	3	(not applicable)
Cold Storage	Computer - Server	5	< 04 Hours	3	<2 Hours
TECHFTP	Computer - Server	5	< 04 Hours	4	(not applicable)
MTSXR01 (Fax Server)	Computer - Server	5	< 04 Hours	3	(not applicable)
MAXACCESS	Computer - Server	5	< 04 Hours	3	(not applicable)
ALTWS001 (Database Server)	Computer - Server	5	< 04 Hours	4	<2 Hours
APPTS3	Computer - Server	5	< 04 Hours	3	(not applicable)
WKST01	Computer - Standalone	5	< 04 Hours	4	(not applicable)
WKST02	Computer - Standalone	5	< 04 Hours	4	(not applicable)

Benefits of a BIA Process

- An effective tool to aid Management on determining Critical Business Functions and Processes
- Effective way to prioritize Resumption and Recovery efforts from a business perspective
- Provide the leverage needed for the support and investment on Business Continuity Management
- Clear understanding between the Business Process and IT Components
- Effective Risk Mitigation Process

Why is BIA Process so critical?

Where to start?...The Risk Pyramid



- Implement new business strategic initiatives
- Provide accurate, timely and complete information that meet stakeholders needs
- Ensure only authorized people have access to information and facilities
- Keep Existing Processes Running and Recovery Capabilities

Business Continuity Regulatory Impact

Sarbanes-Oxley-COSO ¹	FFIEC/OCC ²	GLBA ³	HIPAA/HHS ⁴	ISO ⁵
COSO framework promotes the improvement of quality through effective internal controls	FFIEC Examination Guidelines - Business Continuity Planning Handbook	GLBA Privacy Act emphasis on disclosure of consumer financial information: IT Security of customer financial information in relation to disclosure to third parties Encryption requirements	Health Insurance Portability and Accountability Act 1996 Ensure Confidentiality, integrity, and <u>availability</u> of all electronic protected health information the covered entity creates, receives, maintains and transmits. Protect against any reasonably anticipated <u>threats or hazards</u> to the security or integrity of the information.	International Organization for Standardization is the world's largest developer of standards. The role played by standards is to raise the levels of quality, safety, reliability, efficiency and interchangeability - as well as to provide such benefits at an economical cost.
Business Continuity Control Environment Establish effective Controls Align to Business processes Obtain BC Competence Establish BC Policies & Procedures Control Activities IT Operational controls (i.e. Back-up, Recovery Procedures & Contingency Plans) Monitoring Oversight of Management through risk assessment and performance measures (i.e. testing and risk control metrics)	Business Continuity Risk Assessments Business Impact Analysis BC Plan Development & Maintenance BC Risk Monitoring	Business Continuity Include Customer Information disclosure to BC Third Parties Include Encryption requirements on Recovery Solutions	Business Continuity Administrative Safeguards Security Management Process (Risk Analysis, Risk Management, Sanction Policy) Physical Safeguards (contingency plan, access control and validation procedures) Technical Safeguards (Integrity Controls and Encryption,)	Business Continuity Management Process to maintaining BC throughout the organization BIA & Risk Assessment to identify risk and impact to business interruption Implement Plan to restore critical business operations in required time scales following an interruption Single Framework of BC plans should be maintained Testing & Maintaining of BC Plans

Shared Attendance Discussion

- Current BIA Challenges...???
- Types of BIA Processes in use...???
- BIA Automation Solutions...???
- Any Other Concerns???





Lillibett Machado, MBA, CGEIT, CISM, CBCP, ITIL-BSM

Telephone: 832-724-1005

e-mail: lmachado@fulvenceUSA.com