ISACA
Houston Chapter - Seminar
10-18-2007

"How to Assess your Business Continuity Plan"

fulvencéUSA

Our Service Delivery

P.O. Box 130233 . Houston . Texas . 77219-0233 . 832-724-1005

www.fulvenceusa.com

fulvencéUSA

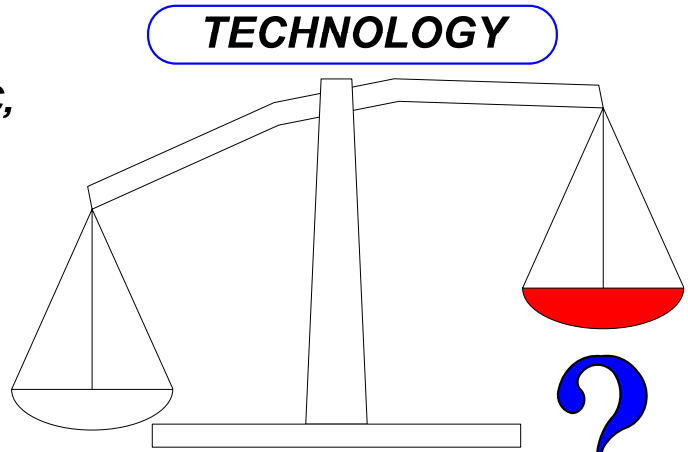
AGENDA

- ✓ **IT Governance & Continuity Risk**
- ✓ **Business Continuity Management**
- ✓ **IT Continuity Controls / Audit Guidelines**
- ✓ **Business Impact Assessment "Starting Point" Exercise**

fulvencéUSA

IT Governance & Continuity Risk
Why Manage IT Risk?

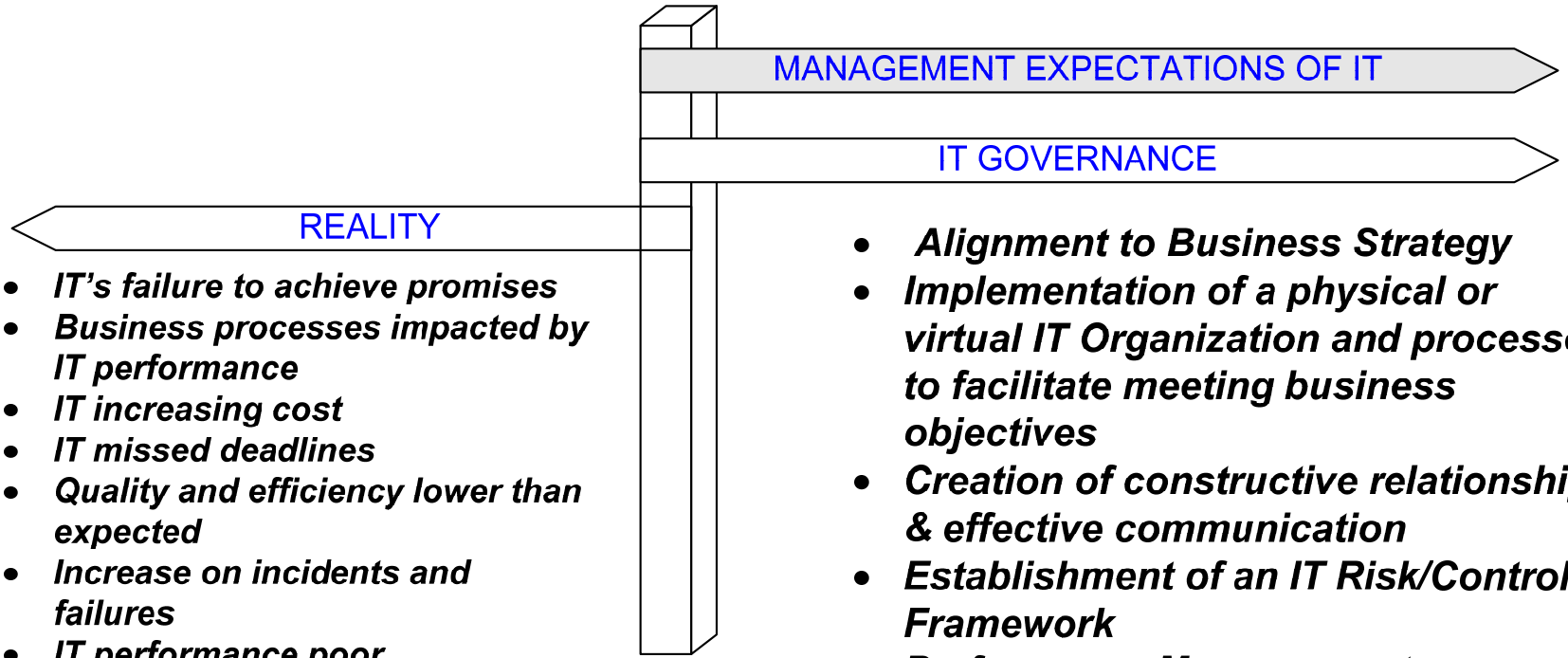
- *To meet the continuous need to sustain the business and new business models*
- *To comply with the increase in regulations (i.e. SOX/COSO, FFIEC, FDIC, BASEL...)*
- *To consolidate IT disciplines overlapping risk management efforts*
- *To promote effective communication and alignment of IT to the Business*
- *To increase operational resilience...for the continuity of the business*
- *To achieve process efficiency to reduce cost and increase service availability and delivery*



Achieving Objectives?
Resilient Enough?
Managing Risk Efficiently?
Cost Efficient?

fulvenceUSA

IT Governance & Continuity Risk Management Expectations



- *IT's failure to achieve promises*
- *Business processes impacted by IT performance*
- *IT increasing cost*
- *IT missed deadlines*
- *Quality and efficiency lower than expected*
- *Increase on incidents and failures*
- *IT performance poor*
- *IT lack of alignment to Business Strategy*

- *Alignment to Business Strategy*
- *Implementation of a physical or virtual IT Organization and processes to facilitate meeting business objectives*
- *Creation of constructive relationships & effective communication*
- *Establishment of an IT Risk/Control Framework*
- *Performance Measurements*

IT Governance .....

Structure

Relationships and Processes

Direction & Control

Achieves Enterprise Goals

Adds Business Value

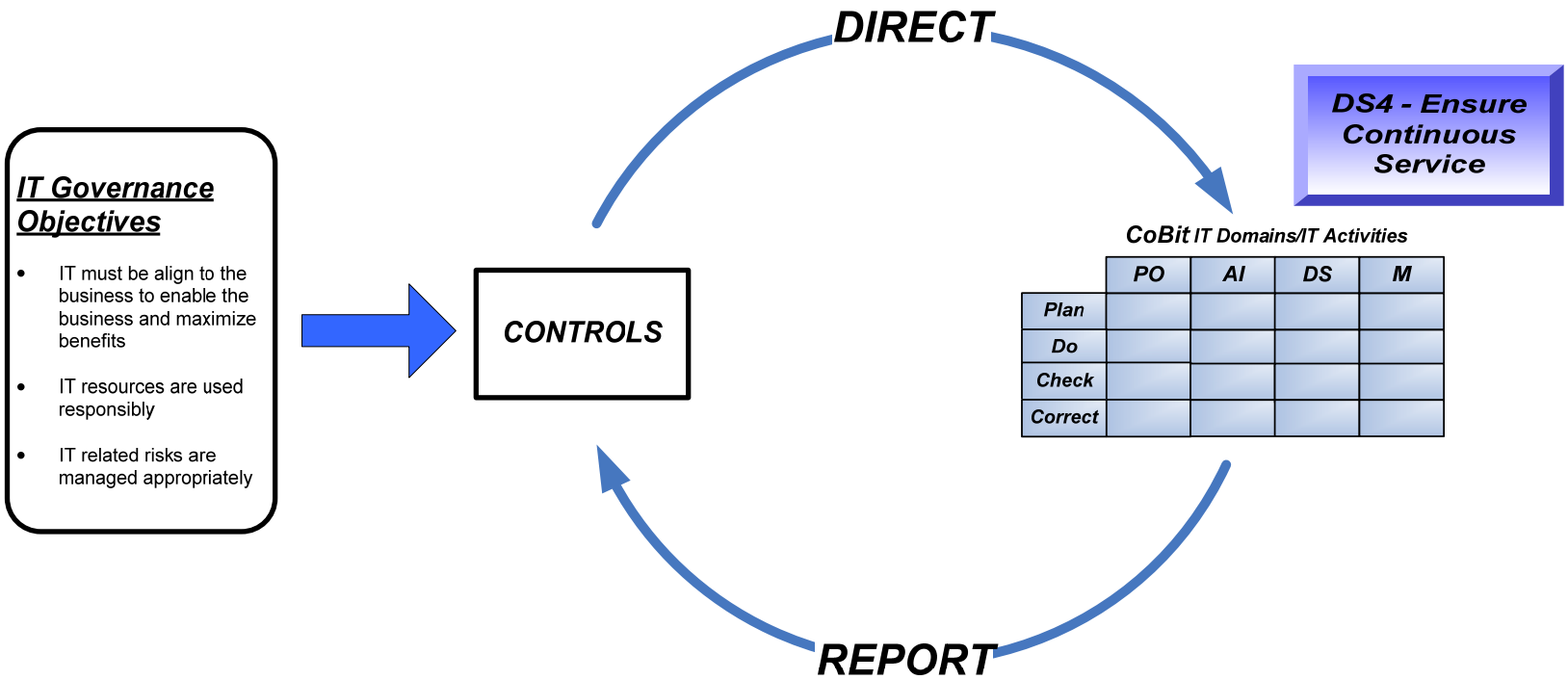
Balances Risk vs. Return

"Over Information Technology"

Allows you to…

- Use IT's enabling capacity for new business models and changing business practices
- Achieve an appropriate return on IT's investment
- Manage ***technology risk***
- Maintain IT's ability to build knowledge
- Reduce/Control IT failures that impact enterprise value and reputation

IT Governance & Continuity Risk
Directs and Controls



AGENDA

- ✓ IT Governance & Continuity Risk
- ✓ Business Continuity Management
- ✓ IT Continuity Controls / Audit Guidelines
- ✓Business Impact Analysis “Starting Point” Exercise

fulvencéUSA

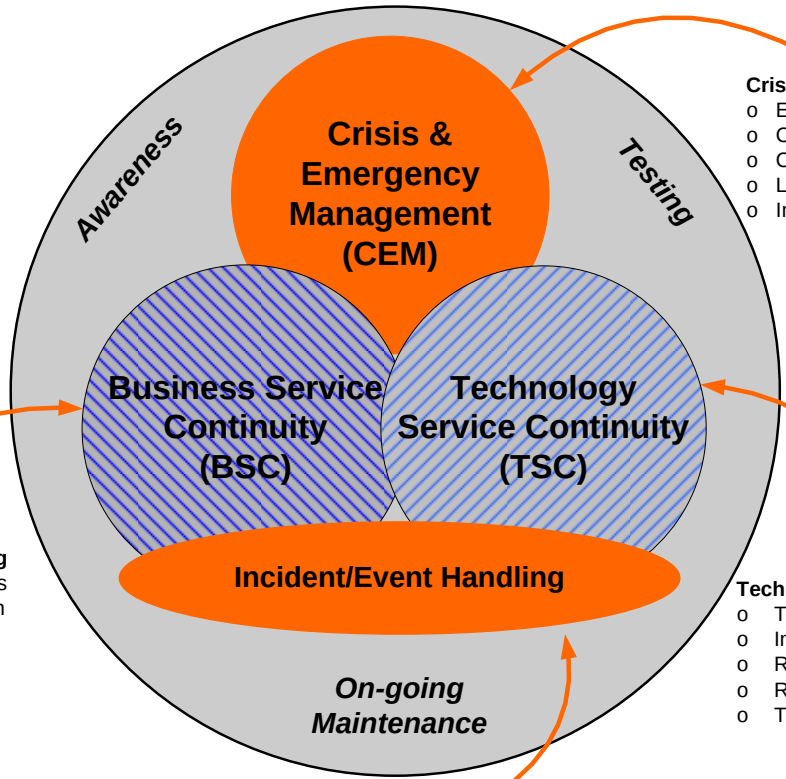
BC Definitions…Confused!!!

- Business Continuity Management
- Crisis or Incident Management
- Disaster Recovery Planning
- Business Resumption Planning
- Technology Continuity Planning
- Resilience & Continuity
- Business Impact Analysis (BIA)

Business Continuity Management FRAMEWORK – "The Three Bubbles"

Enterprise-Wide Approach

- *Business Processes*
- *Operational Risk Mitigation*
- *Business Impact Analysis*
- *Resilience & Continuity Solutions*
- *Regulatory & Standards Integration*



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

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

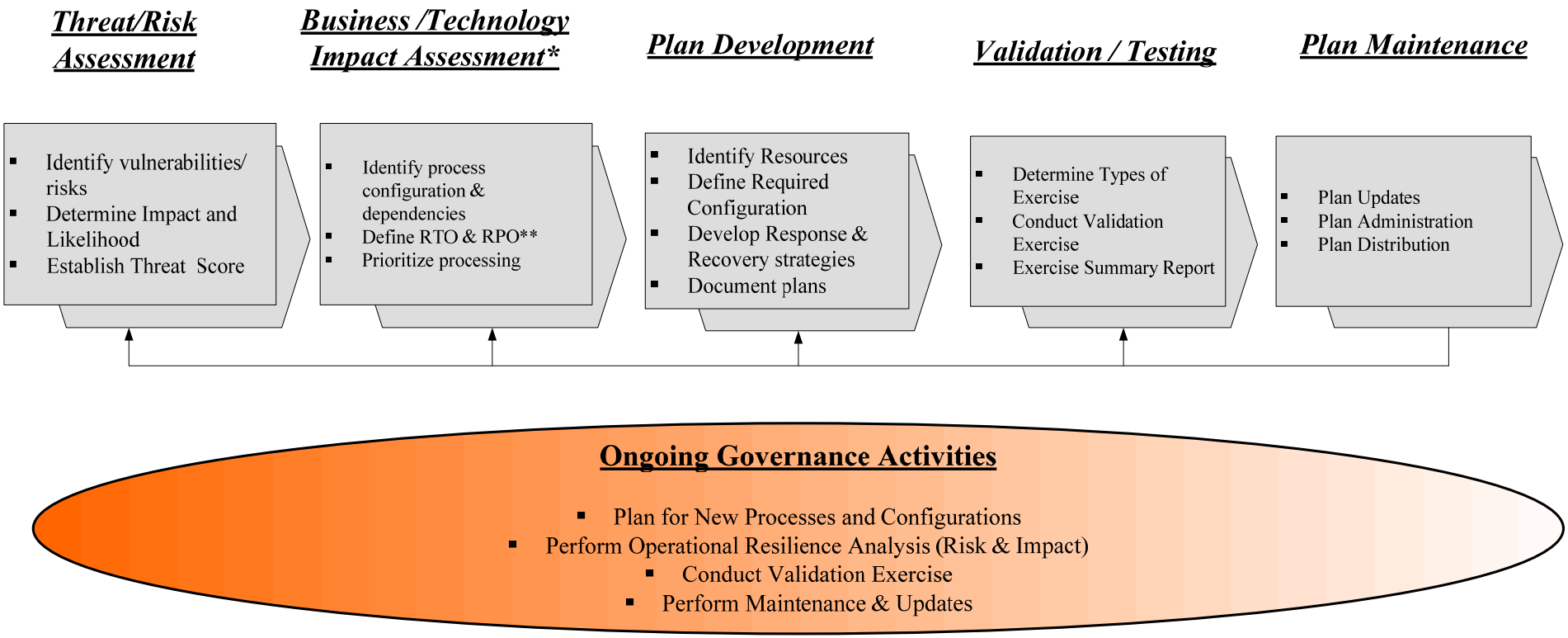
Technology Service Planning
- Technology Service Impact Analysis
- Incident/Event Escalation
- Recovery & Resumption Strategies
- Resource Requirements
- Testing & Awareness

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

fulvencéUSA

Business Continuity Management

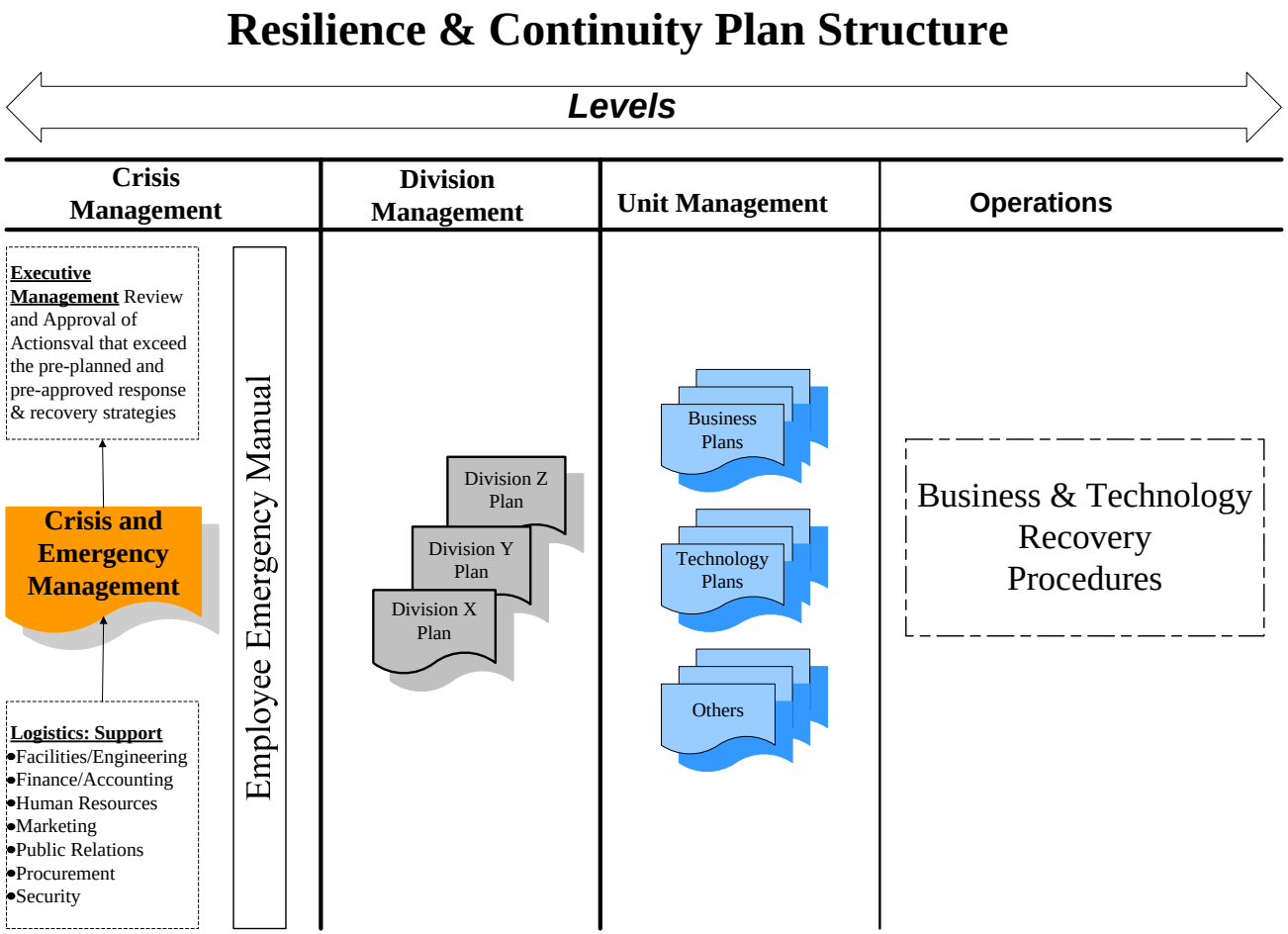
PLANNING PROCESS



Ongoing Governance Activities

- Plan for New Processes and Configurations
- Perform Operational Resilience Analysis (Risk & Impact)
- Conduct Validation Exercise
- Perform Maintenance & Updates

Business Continuity Management
PLAN STRUCTURE



AGENDA

- ✓ IT Governance & Continuity Risk
- ✓ Business Continuity Management
- ✓ IT Continuity Controls / Audit Notes
- ✓Business Impact Assessment “Starting Point” Exercise

fulvencéUSA

IT Continuity Controls and Audit
Ensure Continuous Services - CONTROLS

- Continuity Framework
- IT Continuity Plans
- Critical IT Resources
- Maintenance of the IT Continuity Plan
- Testing the IT Continuity Plan
- IT Continuity Plan Training
- Distribution of the IT Continuity Plan
- IT Services Recovery and Resumption
- Offsite Back-up Storage
- Post Resumption Review

Continuity Framework

- **Assure that a framework has been developed for IT Continuity to support the business with a consistent process**
  - BCM Policy
  - Framework Diagrams
  - IT Strategic Plan – Business Continuity Strategy
- **Assure the framework addresses the organizational structure covering roles, tasks, responsibilities of internal or external service providers, management and customers .**
  - BCM Policy or Plans (Crisis Management, DR or Business)
  - Service Provider Contracts
  - Service Provider's SAS70 Type 1 or 2
- **Assure that rules and structure are available to document, test and execute the Business Continuity/Technology Continuity Plans**
  - **Procedures or Working Templates**

IT Continuity Plans

- **The IT Continuity plans most be design to reduce the impact of a major disruption on key business functions**
  - Recent Risk Assessment
  - Recent Business Impact Assessments
  - Up to date Technology Plan (s)
- **Plans should address requirements for resilience**
  - Business Impact Assessments
  - Evaluate Plan Scenarios and Responses
- **Plans should address Alternate Processing and Recovery Capabilities for critical IT Services.**
  - Business Impact Assessment – Critical Services
  - Evaluate Plan Alternate Locations
  - Alternate Site Assessments

Critical IT Resources

- **Ensure critical items are in the plans and priority has been established**
  - Business Impact Analysis- Process Risk Rating & Resource Item Reliance Rating
- **Assure Regulatory requirements are meet for all critical items**
  - Define enterprise regulations
- **Consider resilience, response and recovery requirements are met for different tiers**
  - Business Impact Analysis-Critical Services RTO

Maintenance of the IT Continuity Plan

- **Change Control procedures are in place to assure plan maintenance and reflects the business requirements**
  - Business Impact Analysis – Business Requirements
  - Review of Change Management Design and Scope
  - Compare Change transactions impacting Recovery or Resumption solutions to assure the plan meets current business solutions

- **Assure procedure and responsibility changes are communicated clearly and in a timely manner**
  - Awareness Program
  - Change Communication Frequency
  - Plan Update and Distribution documents

Testing the IT Continuity Plan

- **Ensure test are performed on a regular basis ensuring IT System effective recovery**
  - BCM Policy
  - Business Impact Analysis – Critical Services/Systems
  - Testing Procedures or Schedules
- **Ensure test results are documented , reported and action plans prepared for remediation**
  - BCM Policy
  - Testing Procedures or Methodology
  - Remediation Action Plans and Schedule – “Lessons Learn”
- **Determine types of testing executed to evaluate testing extent and effectiveness**
  - BCM Policy
  - Testing Procedures or Methodology
  - Testing Plan and Results

IT Continuity Plan Training

- **Training Sessions should be planned and schedule to include key personnel and service providers**
  - BC Policy
  - Training Procedures
  - Training Evidence – Presentations, tabletops, simulations

- **Verify training is performed for remediation done as a result of plan testing or actual event impact**
  - BC Policy
  - Testing Procedures or Methodology
  - Training Evidence – Presentations, tabletops, simulations

Distribution of the IT Continuity Plan

- **Ensure a defined and managed distribution strategy exist**
  - BC Policy
  - Plan Distribution Control List
- **Ensure plans are accessible under any scenario**
  - Threat and Risk Assessment
  - Business Impact Analysis
  - Gather Evidence to determine plan accessibility

IT Services Recovery and Resumption

- **Assure plan includes recovery and resumption of services**
  - Business Impact Analysis
  - Technology Plans
  - Technology Recovery and Resumption Strategy and Procedures
- **Assure activation procedures are in place and current, supporting back-up sites and alternate processing**
  - Activation Strategy in Plans
  - Activation Procedures
  - Compile all Back-up Sites and Alternate Processing Facilities
- **Assure Customers, Service Providers and Business Functions are activated and notified**
  - Business Impact Analysis – List of Service Providers
  - Technology Plans
  - Technology Recovery and Resumption Strategy and Procedures
- **Ensure communication with the Business or Management on IT Recovery Times and Technology Investment**
  - Management or Board Presentation Minutes
  - Management Testing or Training

Offsite Back-up Storage

- **Ensure critical back-up media, documentation and necessary IT resources for recovery and resumption are store Offsite**
  - Back-Up Data & Media Offsite Storage Procedures
  - Business Impact Analysis – Recovery Point Objective (RPO)
  - Operations Daily Log – Back-up frequency and media location
- **Ensure Back-up content meets business requirements**
  - Operations Daily Log – Back-up frequency and media location
  - Offsite Media Log
  - Back-up Equipment Compatibility
- **Ensure management of the offsite storage responds to the data classification policy and the enterprise**
  - Enterprise Data Classification Policy
  - Offsite Data Classification Policy
- **Ensure Offsite premises arrangements are periodically assess, at least annually for content, environmental protection and security**
  - Offsite Assessments
  - Offsite Service Provider Agreement
  - SAS70’s

Post Resumption Review

- **After a disaster IT Management should determine lessons learn or changes to enhance plan and recovery strategies**
  - Incident Summary Reports
  - Management Presentations - Incidents
  - “Lessons Learn” and Remediation Action Plans

AGENDA

- ✓ IT Governance & Continuity Risk
- ✓ Business Continuity Management
- ✓ IT Continuity Controls / Audit Notes
- ✓Business Impact Assessment “Starting Point” Exercise

fulvencéUSA

Business Impact Analysis (BIA)

BIA is a process designed to:

- identify critical business functions and workflows,
- determine the qualitative and quantitative impacts of a disruption,
- prioritize and establish recovery time objectives and recovery point objectives.

Business Impact Analysis – Key Functions

Process Impact Assessment...

- Plan for highest Probability/Damage Threats
- Define and understand your Business Processes
- Use “architecture diagrams” to select configuration items
- Understand your dependencies
- Determine process work schedule and peak periods

Process Analysis…

- Determine your process “Recovery Time Objective (RTO)” by threat for each process

RTO – Maximum time a business process can be unavailable before adversely affecting your business objective.

Business Impact Analysis – Key Functions

Configuration Item Analysis…

- Determine your “process” Configuration items
- Determine the impact of each item to your process objective
- Determine the “Recovery Point Objective (RPO)” for all items that contain data

RPO – Point in time in which data most be restore after an outage. Critical for the development of your recovery and back-up strategy.

fulvencéUSA

Q & A

Lillibett Machado
Principal/Directive Consultant
Cellular: 832-724-1005

P.O. Box 130233 . Houston, TX 77219-0233
www.FulvenceUSA.com