

Managing a Business Continuity Management Program

Presented by

Randall J. Till, MBCP
Till Continuity Group

ACP Chapter Meeting
Orange County Chapter
June 15, 2011



Business Continuity Session

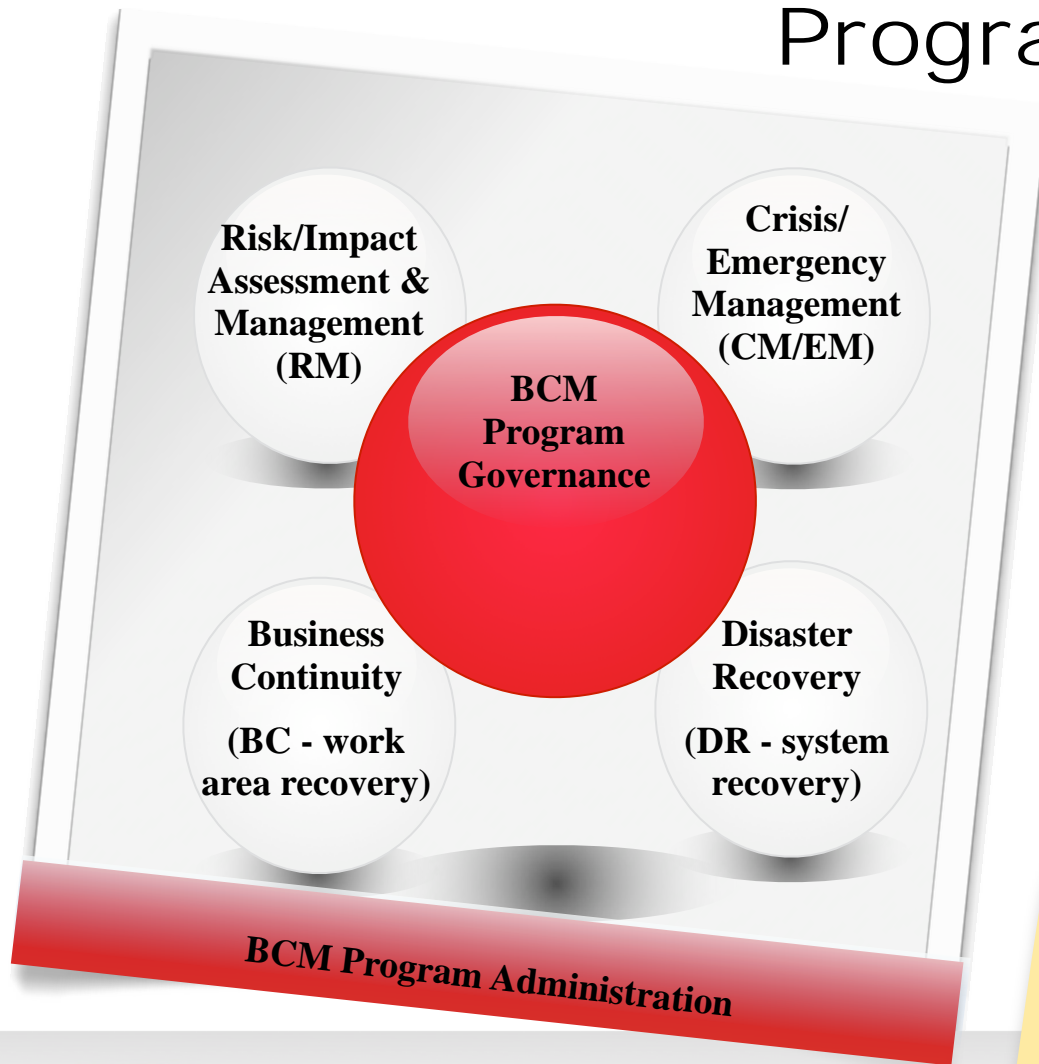
Purpose: Discuss the core components of a BCM Program and engage in discussion around the practices and challenges.

Components:

- Manage -- BCM Program Governance
- Assess -- Risk Assessment and Business Impact Analysis
- Plan - Crisis Management, Business Continuity and Disaster Recovery
- Validate - Testing, Exercises and Measurement
- Maintenance - Maintaining information, plans and readiness

Objective: To generate questions initiating meaningful dialog and conversation.

Business Continuity Management (BCM) Program



- ✓ Each organization is unique
- ✓ Different levels of responsibility
- ✓ Different levels of maturity

Goal: A visible, adequately-equipped program that is compatible with the organization's culture and sustainable for the long-term.

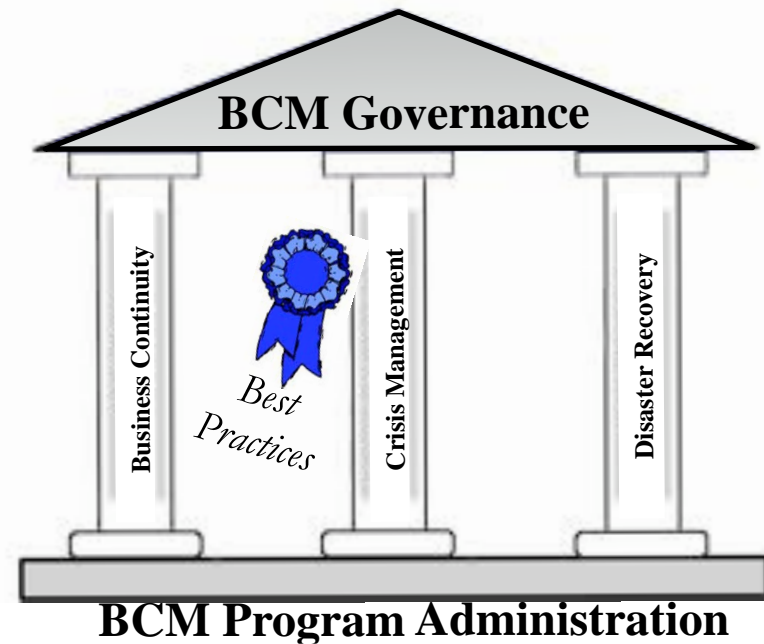
Terminology
for today's
discussion 😊

BCM Approach



**Plan To Pass Audits &
Meet Regulatory
Compliance**

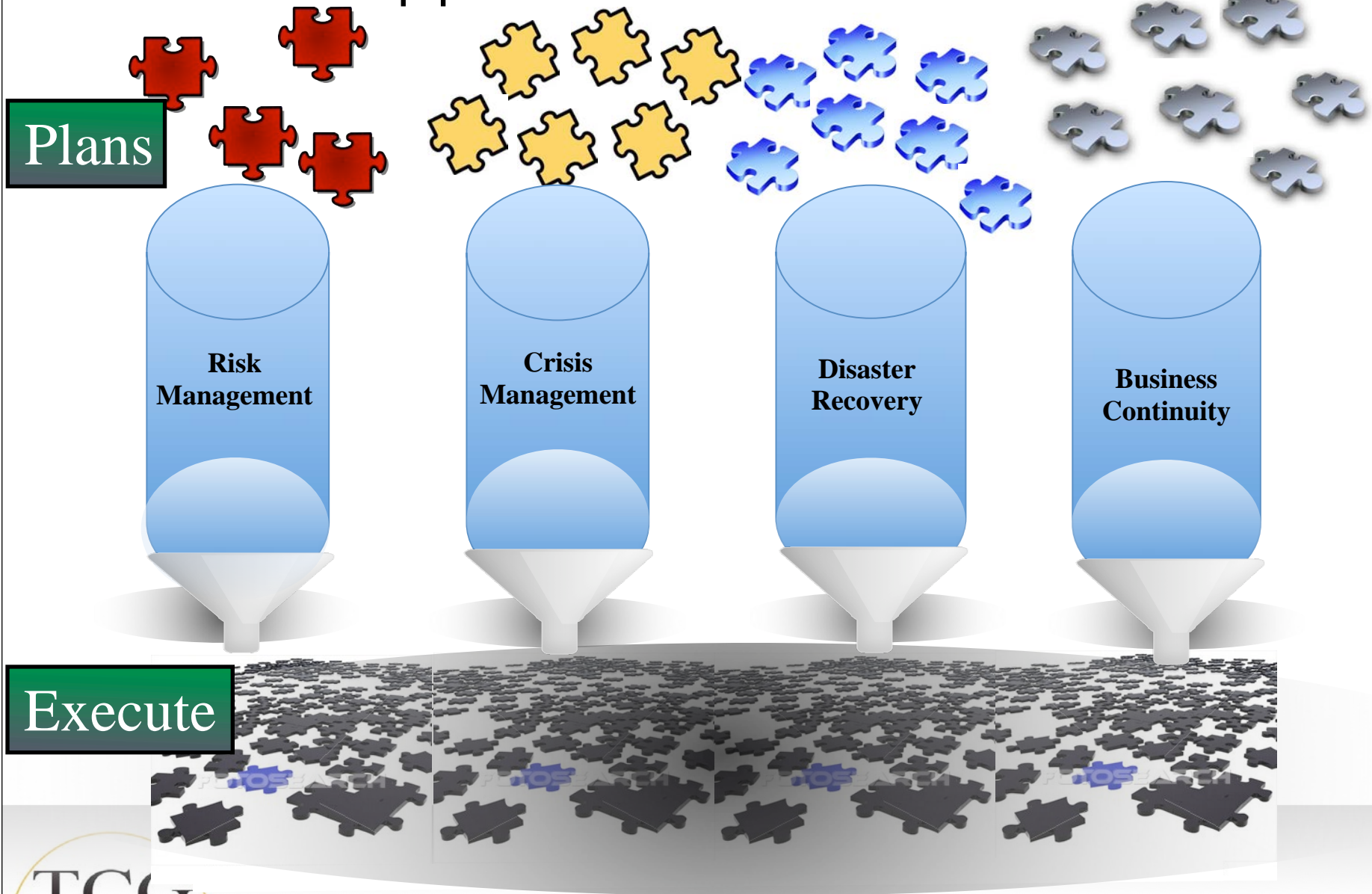
✓ **Poor Investment**



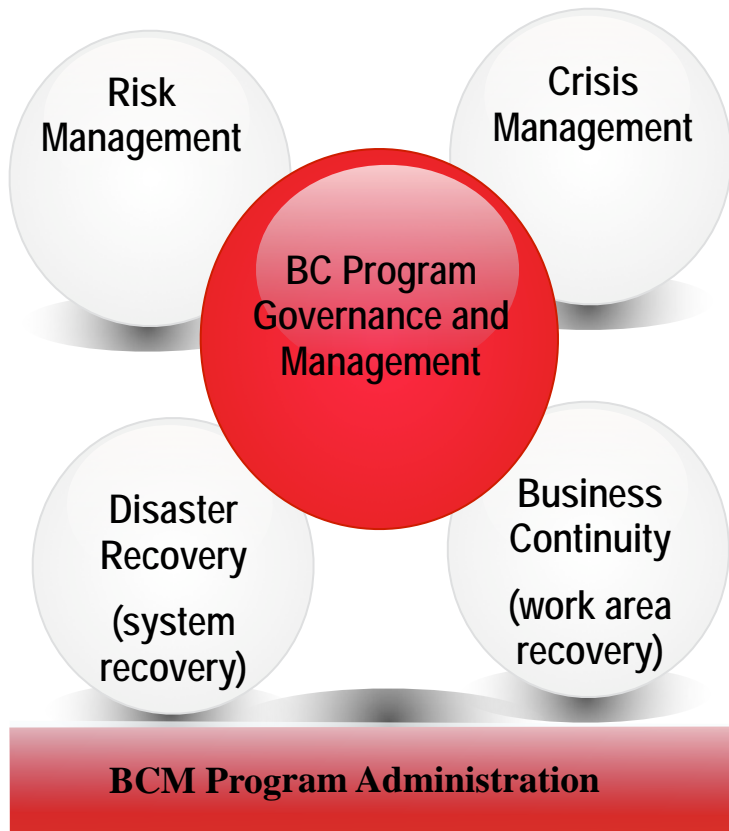
**Plan to Address Risks,
Protect Assets &
Sustain Operations**

✓ **Valuable Investment**

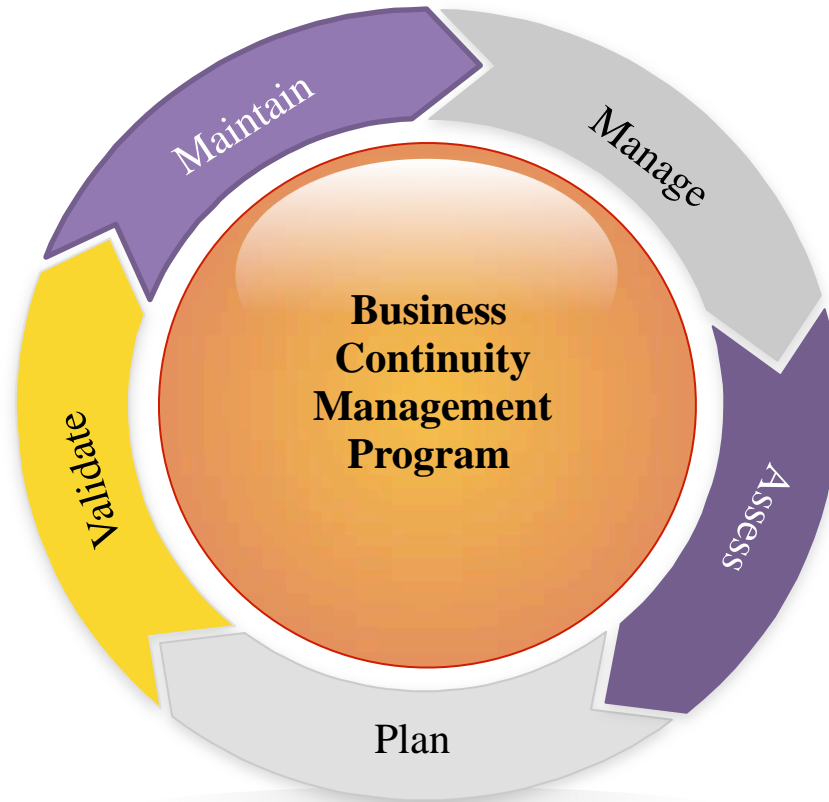
BCM Approach - Siloed Practices



Business Continuity Management (BCM)

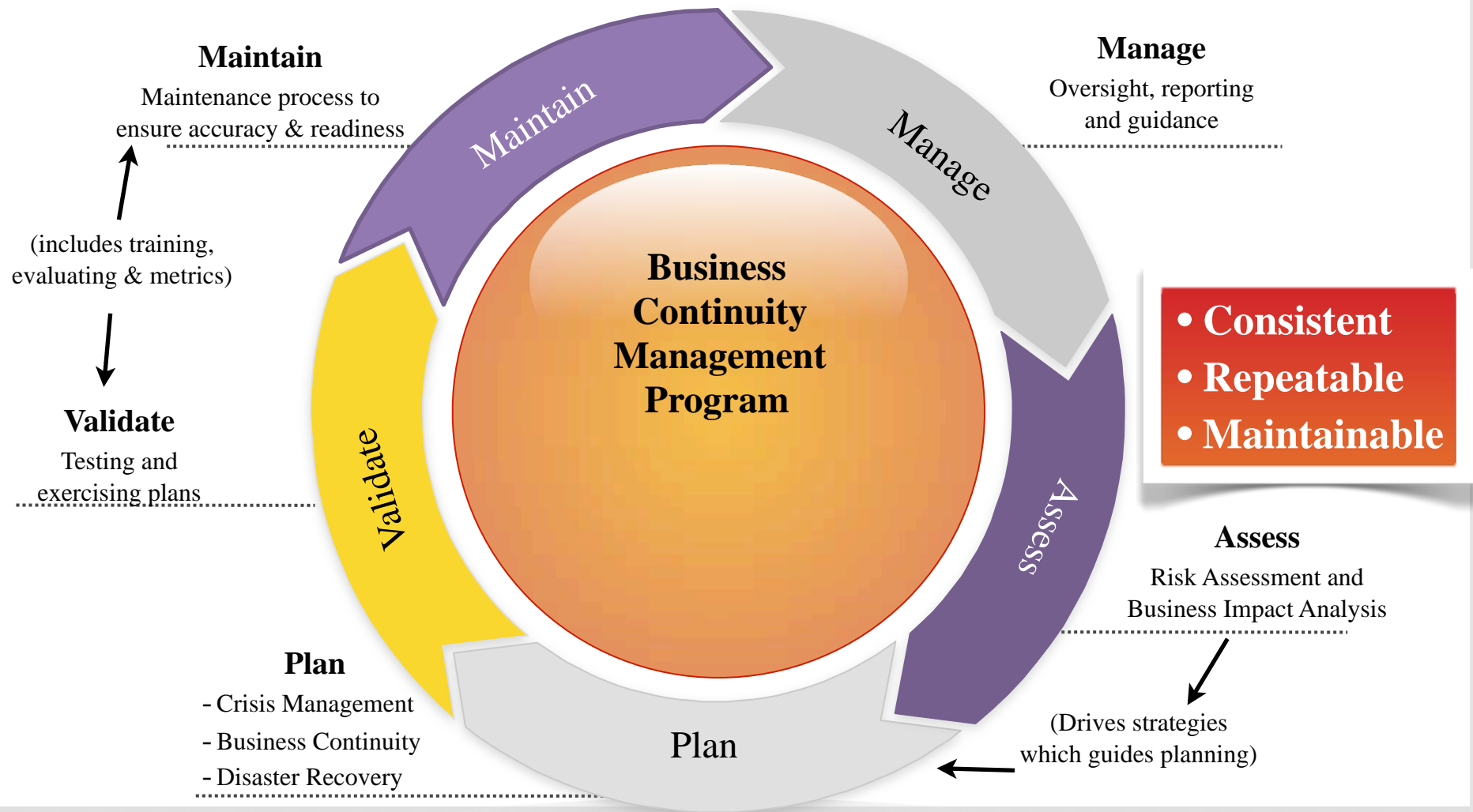


BCM Model
"What"



BCM Planning Cycle
"How"

Business Continuity Planning Cycle



BCM Program Governance



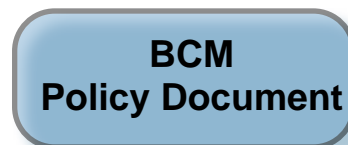
- ✓ **Ownership**
- ✓ **Responsibility**
- ~~✓ **Commitment**~~
- ✓ **Engagement**

What Level ?

- C-Level
- Executive Team
- Senior Managers
- Key Functional Managers



- ✓ **Expectations**
- ✓ **Metrics**
- ✓ **Reporting Structure**



- ✓ **Policies & Standards**

BCM Planning Organization

Ownership

Corporate Headquarters

IT Headquarters

Europe

Asia Pacific

Latin America

Coordination

Regional Coordinators
(Secondary)

Finance

Marketing

Sales

Customer Services

HR

Legal

IT

Division Coordinators
(Primary)

Facilitation

Business Continuity
Planners

Business Continuity
Planners

CM/EM
Plans

BC
Plans

DR
Plans

Discussion Point - Governance

How is BCM structured within your organization?

- Location within the organizational, number of people supporting BCM?
- Do you have formal BCM Policy and standards within your organization?

How are regulations/standards driving your BCM Program?

- Have you been audited?

Do you have a BCM Steering Committee?

- What level in organization, frequency, level of engagement?

How are BCM metrics reported to BCM Steering Committee?

- What level and type of measurement?
- How does it drive or impact BCM?

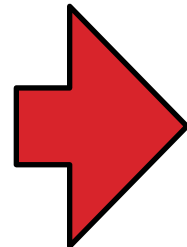
What's been the impact of the economic downturn on the BCM?

What are the issues or questions you have regarding BCM Governance?

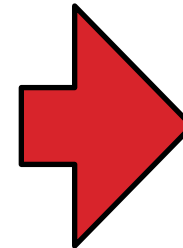
Risk Assessment and Mitigation



**Threat
Identification**



**Controls
Assessment
& Business
Risks**



**Risk
Tolerance &
Mitigation
Steps**

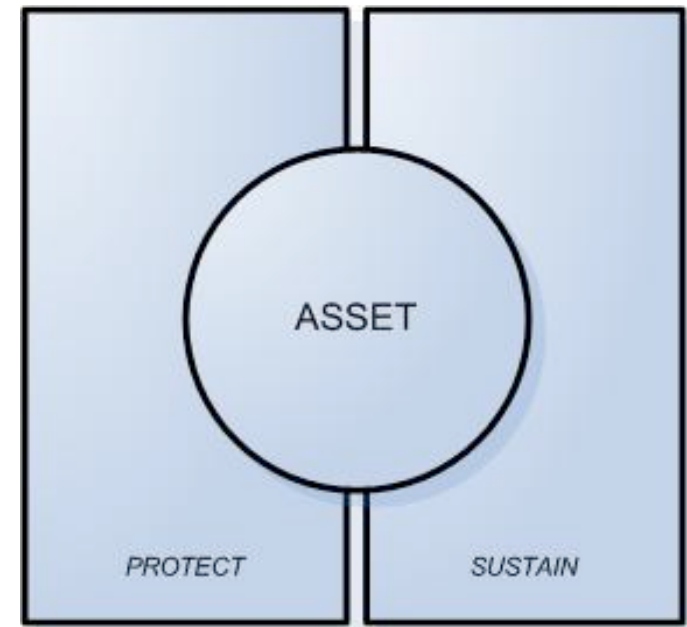
- Business Disruption
- Threats to the Business

- Risks to the Business
- Business Impacts (BIA)

- Risk Appetite
- CM, BC and DR Plans

Holistic Approach to Managing Risks

- Organization is dependent on the productivity of Key Assets:
 - People
 - Information
 - Technology
 - Facilities
- Each asset must be protected and sustained

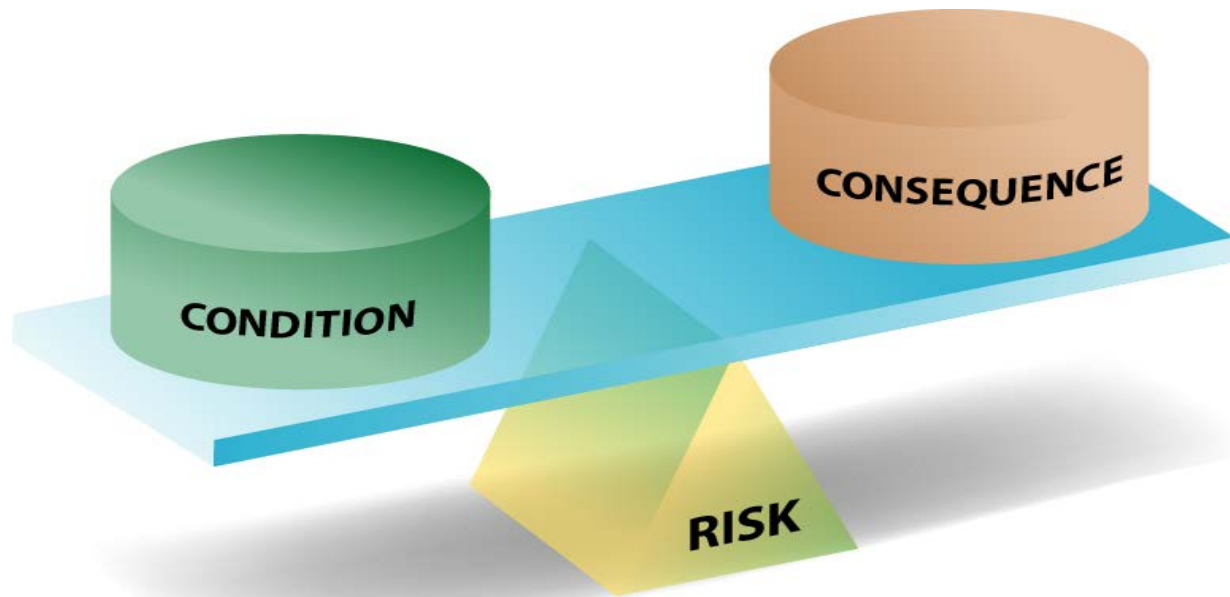


Condition Consequence

Two-sides to Managing Risks



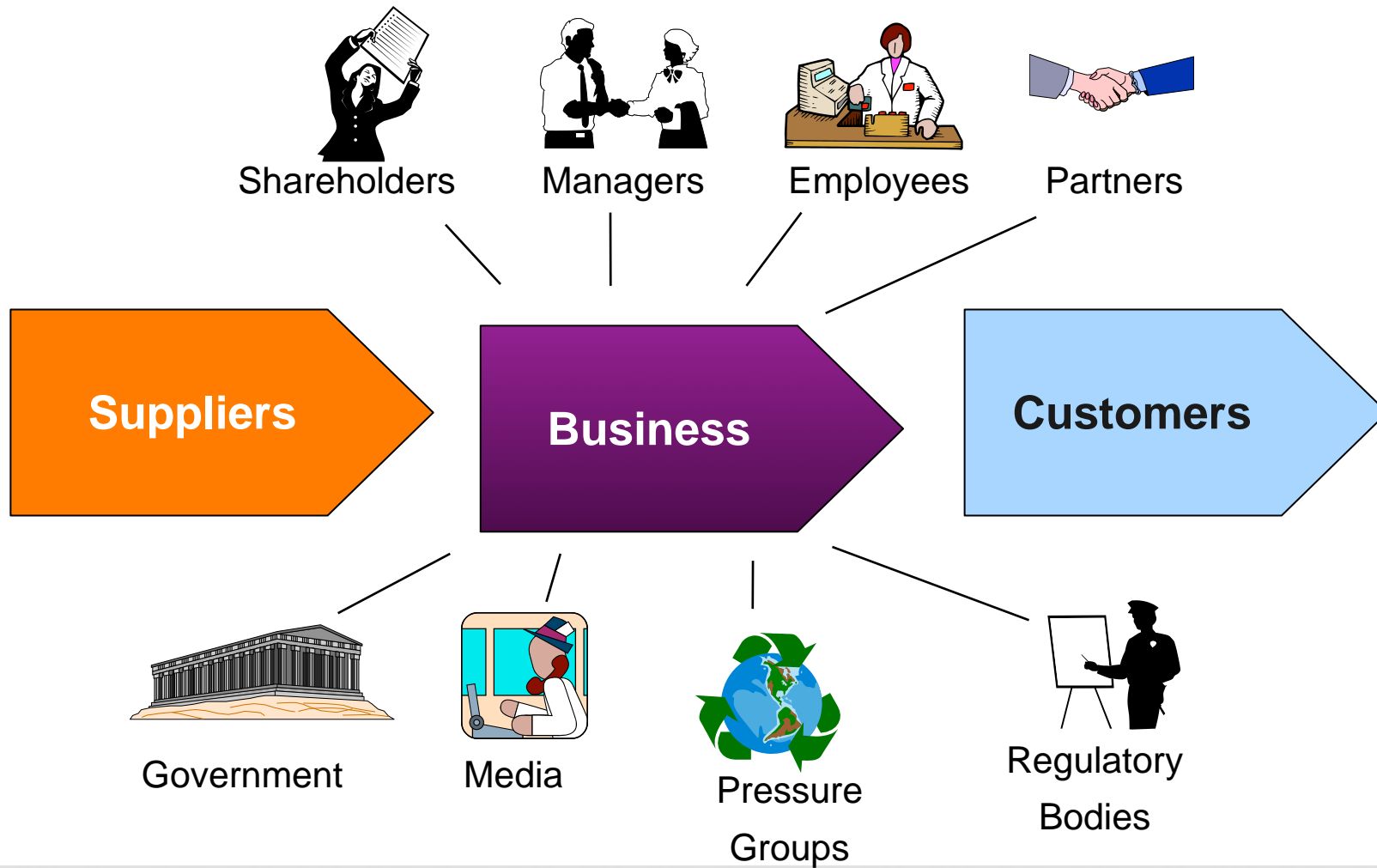
Limited
Funding



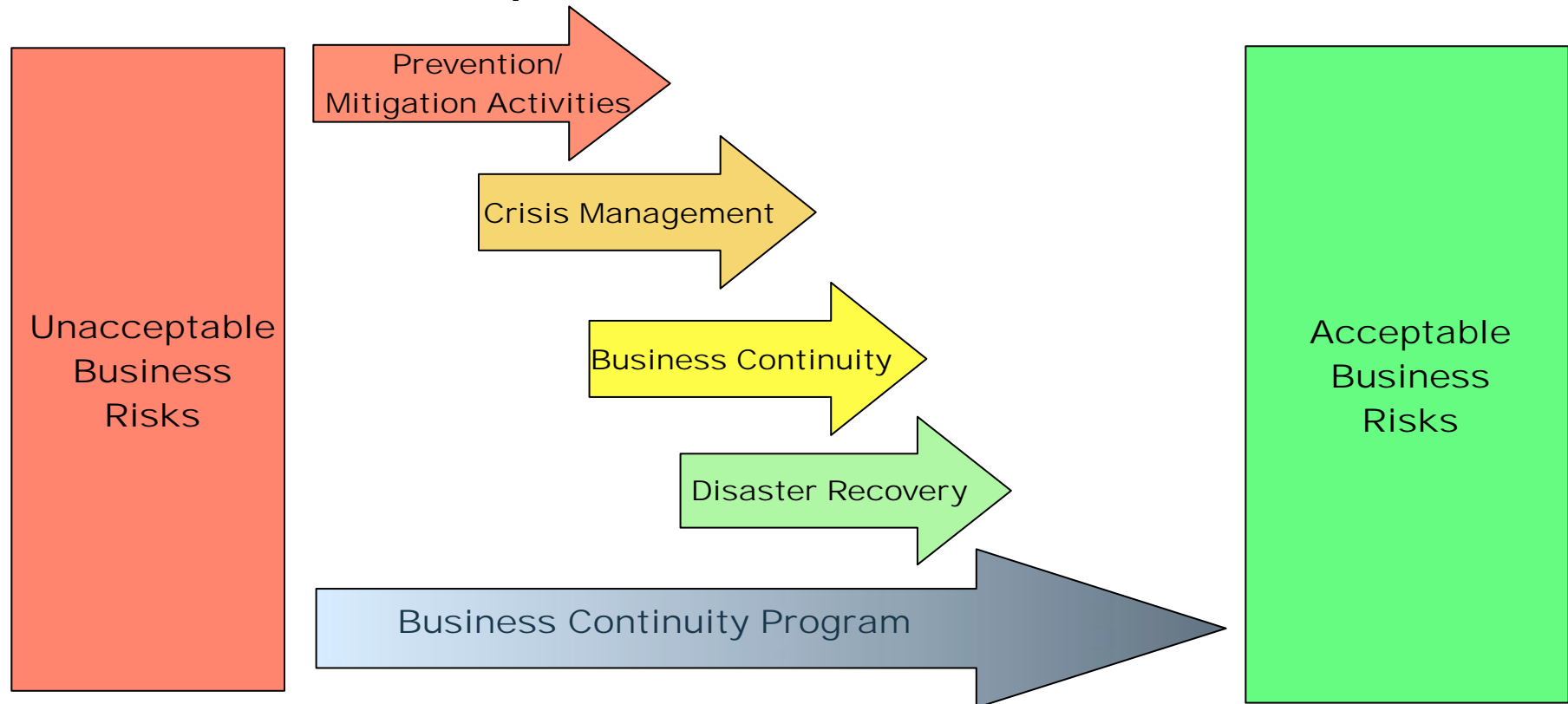
Mitigate risks from
happening

Manage the impacts
of events

Understand the Supply Chain



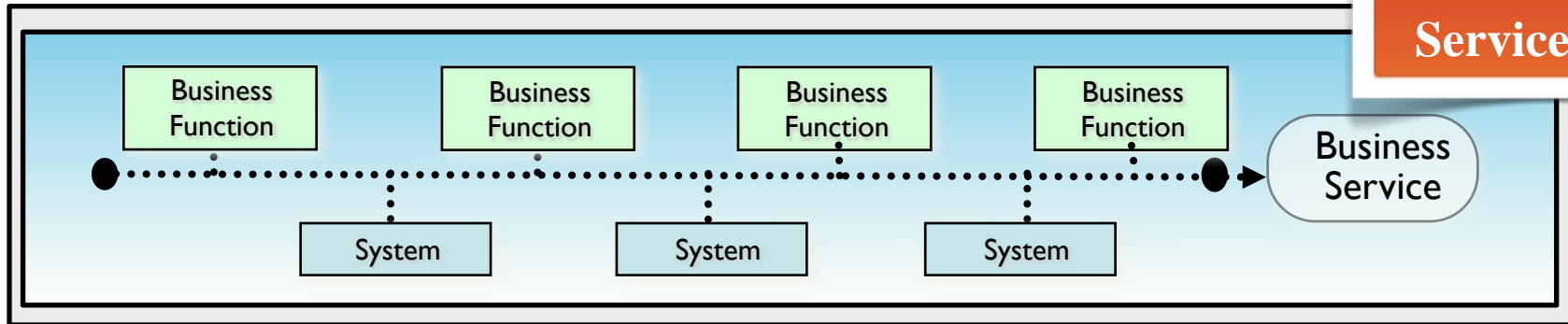
Role of Business Continuity in Managing Operational Risks



Every company has Business Risks; we must be able to determine the acceptable level of Risks.

Business Impact Analysis (BIA)

How critical is the Business Service?



Business Impacts:

- Operational
- Financial
- Customers
- Reputation
- Legal/Regulatory

Impacts Over Time:

- Immediate
- 0-8 hours
- 8-24 hours
- 24-48 hours
- 3-7 days
- >7 days

Criticality Factor:

- Max. allowable downtime
 - RTO - Recovery Time Objective
- Max. allowable loss of data
 - RPO - Recovery Point Objectives

Valuable Strategic Information



Business Impact Analysis (BIA)



✓ **BIA Data Storage & Utilization**

Valuable Strategic Information

BIA Approach

- **Surveys**
- **Interviews**
- **Workshops**
- **Tools**
- **Combination**

✓ **Repeatable Consistent Process**

Discussion Point - Assessment

How are risk assessment performed within your organization?

- Who has responsibility, how are results applied?
- What is BCM role in RM? How does it interface with ERM?
- Do risk assessment drive effective mitigation results?
- Do you manage business risks associated with continuity of operations?

How is BIA process conducted within your organization?

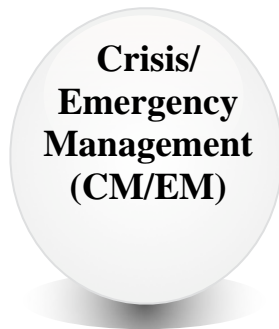
- Business level, technical level or both?
- How often are BIAs performed? How are new business functions/systems included?
- Are tools used to conduct BIAs? Do you use surveys, interviews, workshops?
- How are BIA results incorporated into the planning documents?
- Are BIA results accurate?

Plan - BCM Planning Processes



- **Consistent**
- **Efficient**
- **Repeatable**
- **Automation**

Crisis/Emergency Management (CM/EM)



Management of incident

- **Assessment**
- **Business perspective**
- **Notification & Assembly**
- **Communications**
- **Decisions - Activation**

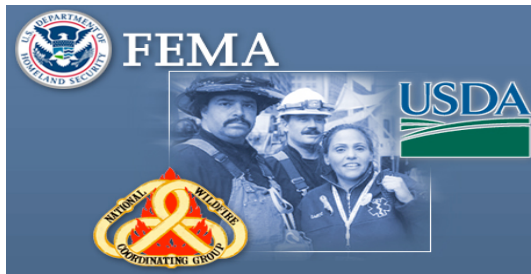


Emergency Response Life Safety - First Response



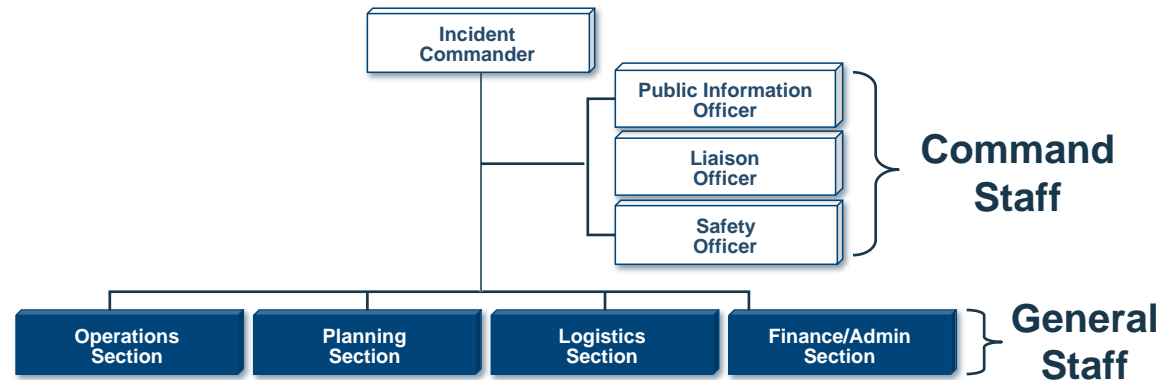
Crisis Management

Crisis/Emergency Management



National Incident Management System (NIMS)

- ✓ Proven
- ✓ Documented
- ✓ Best Practice



CM Organization & Plans

- ✓ Enterprise-wide
 - ✓ Assign responsibilities
 - ✓ Setup Command Centers
 - ✓ Train people
 - ✓ Practice roles and procedures

Crisis Management Strategies

Office Type	Crisis Management Team Assigned*
Corporate and Headquarter Offices	<ul style="list-style-type: none"> - Corporate Incident Response Team (CIRT) - Local Incident Response Teams (LIRT) - Initial Assessment Teams (IAT) - Command Center Sites (2-3)
Regional and Select Offices (Offices with significant # of people/operations)	<ul style="list-style-type: none"> - Local Incident Response Teams (LIRT) - Initial Assessment Teams (IAT) - Command Center Sites (1-2)
Smaller Offices	<ul style="list-style-type: none"> - Initial Assessment Teams (IAT)

* Based on NIMS Structure

Crisis Management Planning Cycle

Deliverables	Headquarter Offices CIRT/LIRTs	Regional/Key Offices LIRTs	Smaller Offices IATs	Due Dates
IAT Training	1	1	1	Mar-Jul
IAT Notification Test	3	1-2	1	Mar, Jun, Sept
IAT Tabletop Exercise - Self Conducted	2	1-2	1	May-Sept
CIRT/LIRT Functional Group Training	1	1	0	Apr-Sept
CIRT/LIRT Notification Test	2	2	0	During exercises
LIRT Scenario Based Exercise - Self Conducted	0	1	0	May-Aug
CIRT/LIRT Scenario Based Functional Exercise	1	0	0	NY - 8/30 Dallas - 04/15 SF - 10/20

Discussion Point - Planning

Have you established an effective CM/EM plan?

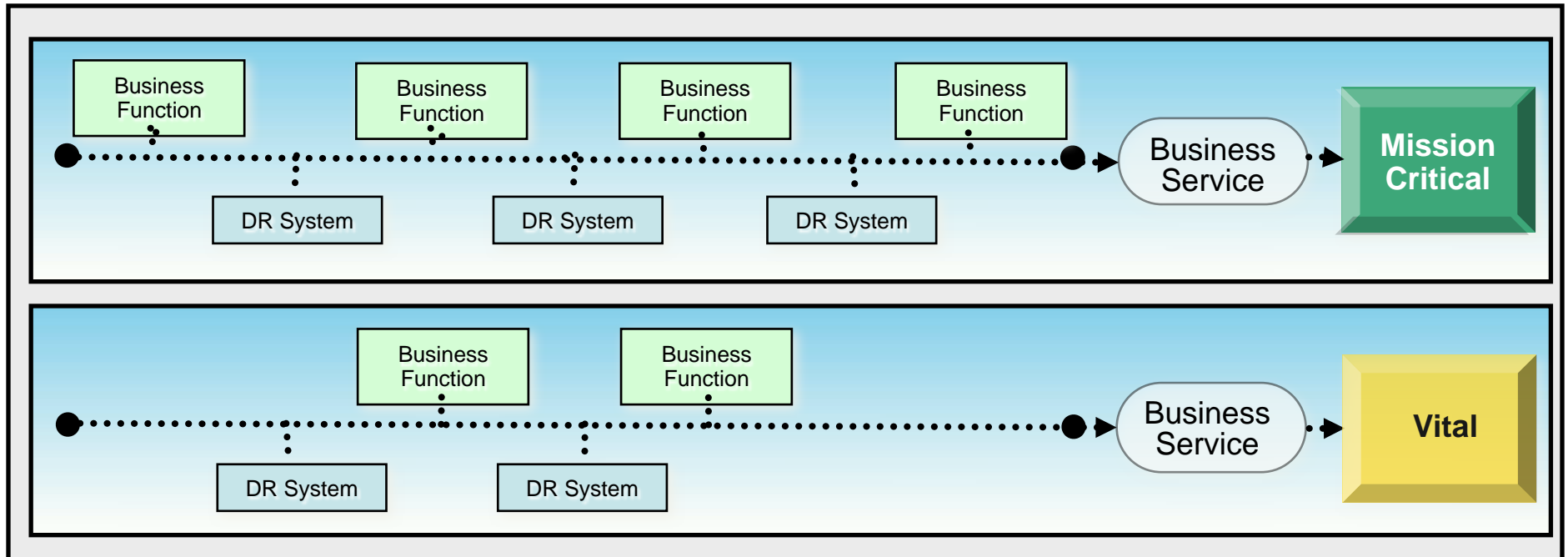
- Enterprise-wide?, NIMS Methodology? Is Management engaged/prepared?
- How often do you test/exercise your CM/EM plans? How often and how extensive? Do you measure your CM exercises or plans?
- Do you have a notification tool? Is it used for EM/CM, BC and DR?

Do you have transition process to move from day-to-day problem solving into crisis Management?

Does Executive Management have a role in the EOC?

What are the issues or questions you have regarding EM/CM?

Business Service Approach



Assign Plans to Business Services

✓ Business focus

✓ Plan integration

✓ End-to-end recovery

Assign Criticality to Business Services

Business Continuity Planning



✓ **Business service**

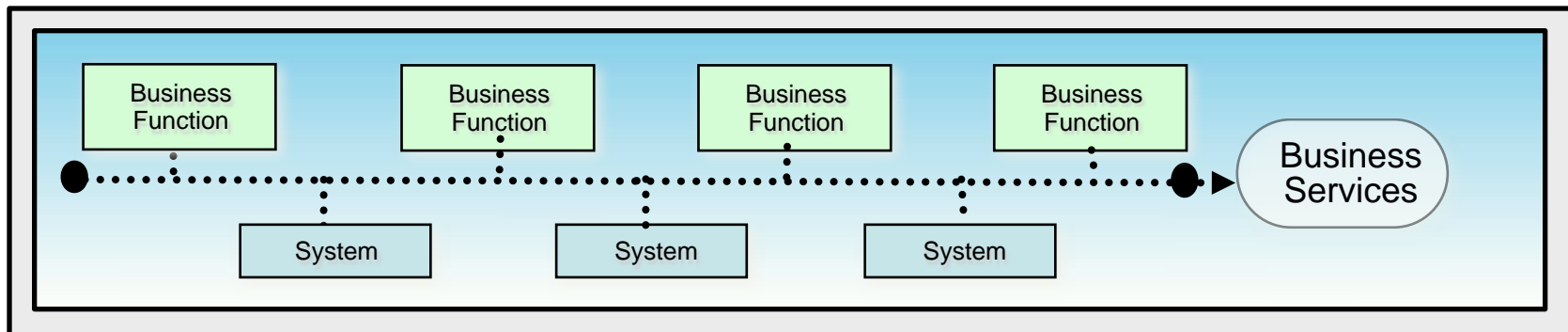
✓ **People**

✓ **Business function**

✓ **Processes & procedures**

✓ **Department**

✓ **Information**



✓ **Systems/applications**

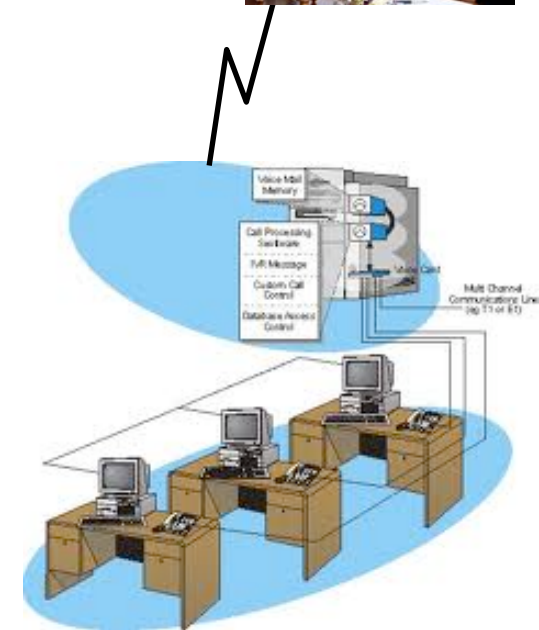
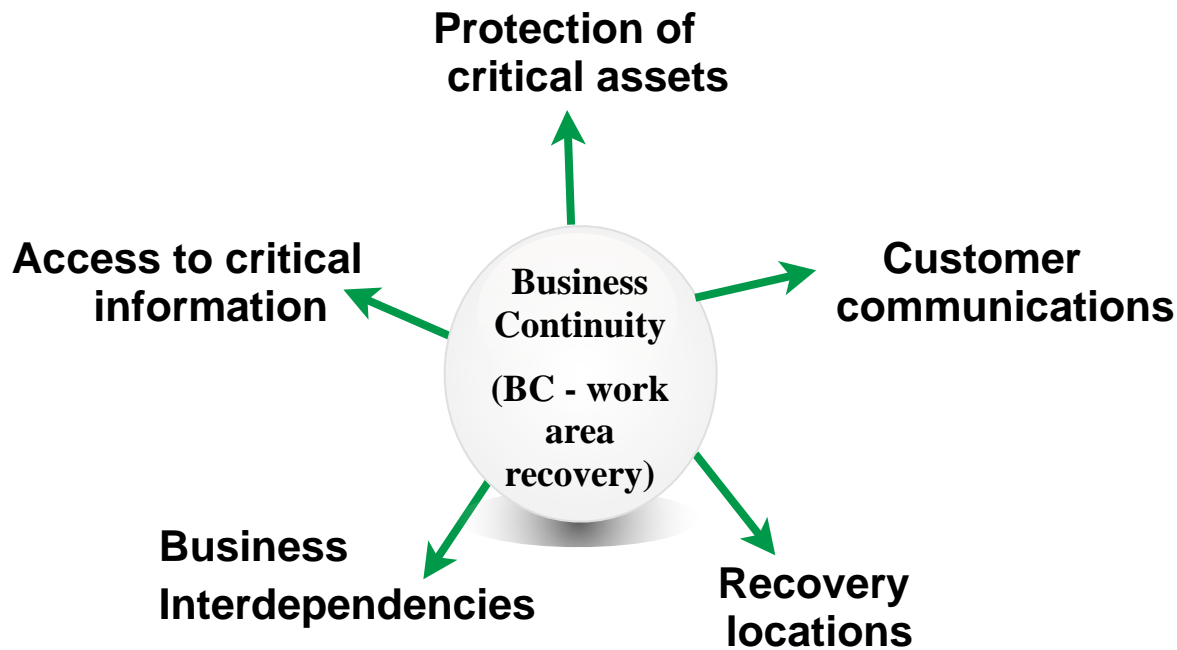
✓ **Customers**

✓ **Technology**

✓ **3rd parties/vendors**

✓ **Dependencies**

Business Continuity Planning



✓ **Business process analysis**

✓ **Process improvement**

✓ **Office Infrastructure**

Business Continuity Strategies

Office Type	BC Planning Levels
Corporate/Core Offices*	– BC planning at business function level
Regional and Select Offices	– BC planing at department level
Smaller Offices	– BC planing at office level
Plan Criticality	Recovery Times and Facilities
Essential Plans*	<ul style="list-style-type: none"> – Critical business functions RTO < 7 days – Recovery facilities pre-established – Detailed plans by functions
Deferred Plans	<ul style="list-style-type: none"> – Less critical business functions >7 days) – No recovery facilities established – High-level plans by function/depart.

*** = Risk Appetite**

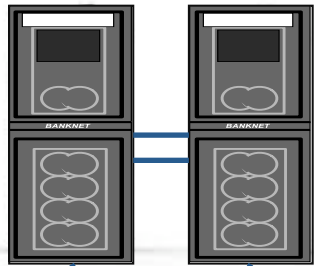
Business Continuity Planning Cycle

Deliverables	Ess	Def	Core	Key	Small	Start Date	End Date
Business Impact Analysis (BIA) Review	x	x	Y	Y	Y	1-Mar	31-Mar
BIA Sign-off by Business Owner	x		Y	Y	Y	1-Mar	31-Mar
Plan Roster Review/Update	x	x	Y	Y	Y	Jan, Apr, Jul, Oct	
Plan Review/Update	x	x	Y	Y	N/A	1-Apr	30-Jun
Business Continuity Manual Review/Update			N/A	Y	Y	1-Apr	30-Sep
Work From Home Validation	x		Y	Y	Y	15-Mar	31-Jul
Team Activation Exercise	x	x	Y	Y	Y	1-Apr	30-Sep
Plan Walkthrough Exercise	x	x	Y	Y	N/A	1-Apr	30-Sep
Business Recovery Site Exercise	x		Y	N/A	N/A	Office-1: Jun 21/Sep 13 Office-2: May 17/Aug 7 Office-3: Jun 1/ Nov. 22	

Disaster Recovery (DR) Planning

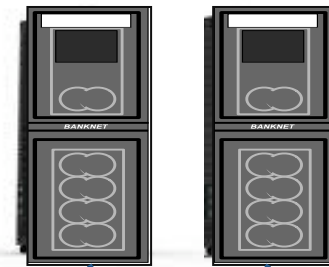
Disaster Recovery
(DR - system recovery)

Primary Site



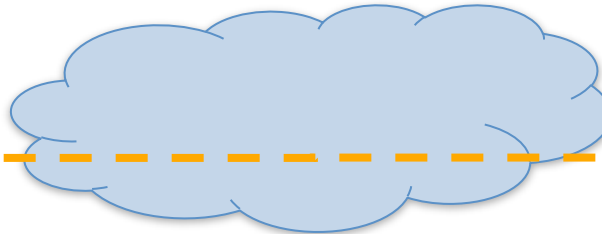
Cost Reductions

Alternate Site



DR Strategy

Shared Disk



Shared Disk



DR Testing



Networks

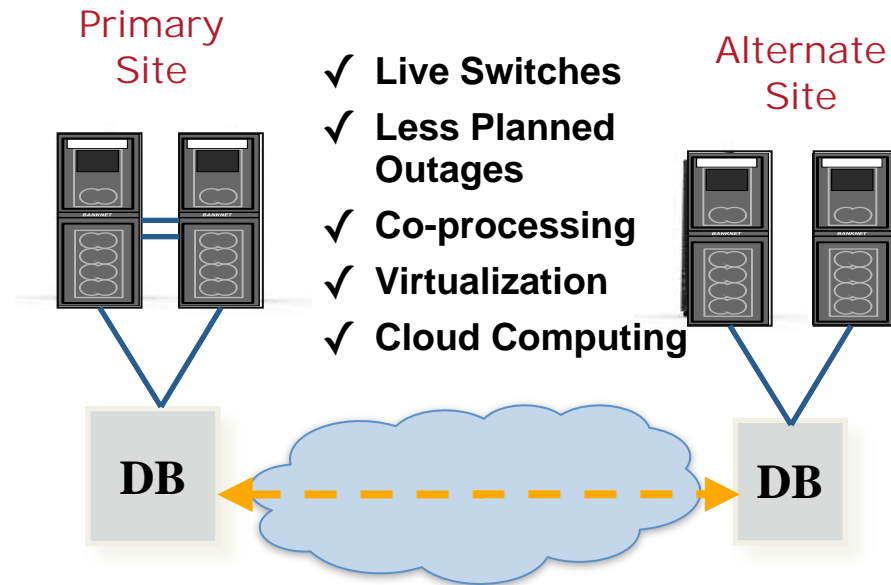


Data Backup

Disaster Recovery Planning

RTO = 0
RPO = 0

- ✓ Lower recovery objectives
- ✓ Less loss of data

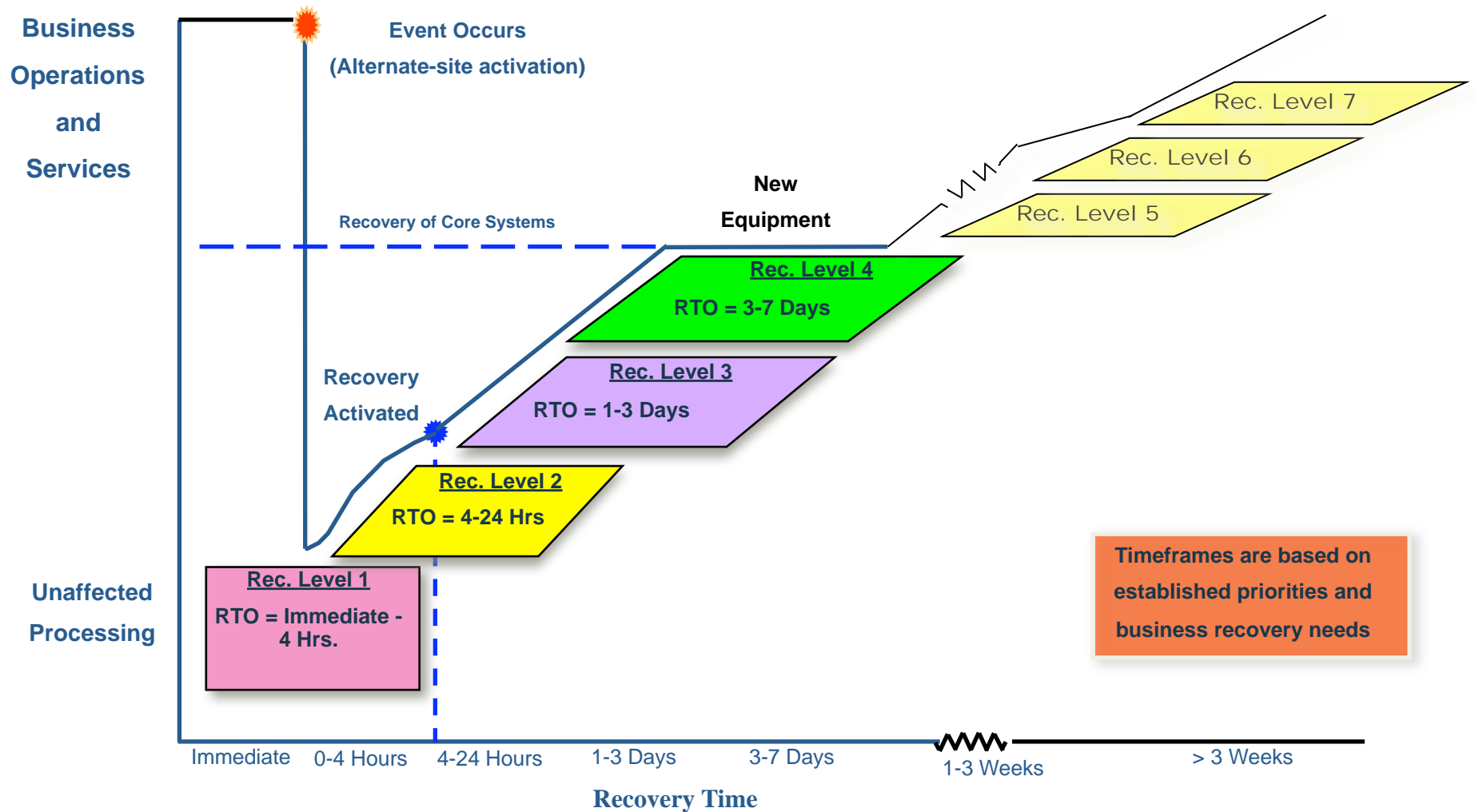


- ✓ Improve system design
- ✓ Utilize DR resources
- ✓ Enhance operating flexibility

Disaster Recovery Strategies

Data Centers	Planning & Exercises
Primary Data Center (Internal Control)	<ul style="list-style-type: none"> - Full DR plans Tier 1&2 systems - Full functional exercises Tier 1 systems
Co-location Data Center	<ul style="list-style-type: none"> - DR plans for Tier 1&2 systems - Coordinated DR exercises with provider
Outsourced Processing	<ul style="list-style-type: none"> - DR plans oversight and DR test evaluation
DR Plan Criticality	Recovery Times and Facilities
Tier 1 Systems	<ul style="list-style-type: none"> – Critical systems RTO = 0-3 days – Hot recovery site established
Tier 2 Systems	<ul style="list-style-type: none"> – Critical systems RTO = 4-14 days – DR plans developed, Warm recovery site
Tier 3 Systems	<ul style="list-style-type: none"> – Critical systems RTO = >14 days – No recovery site established

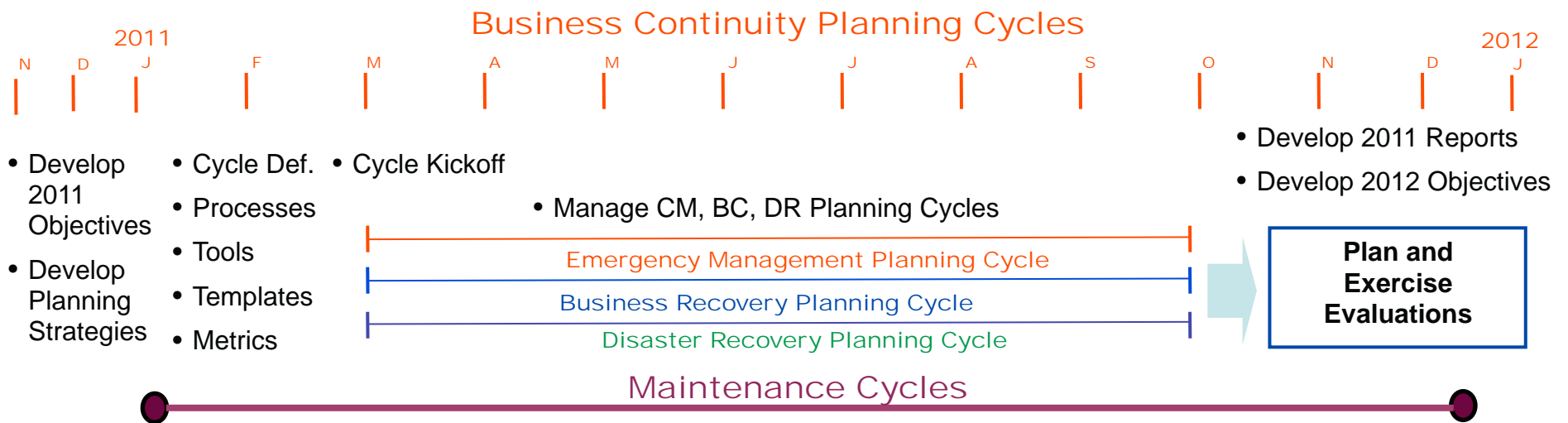
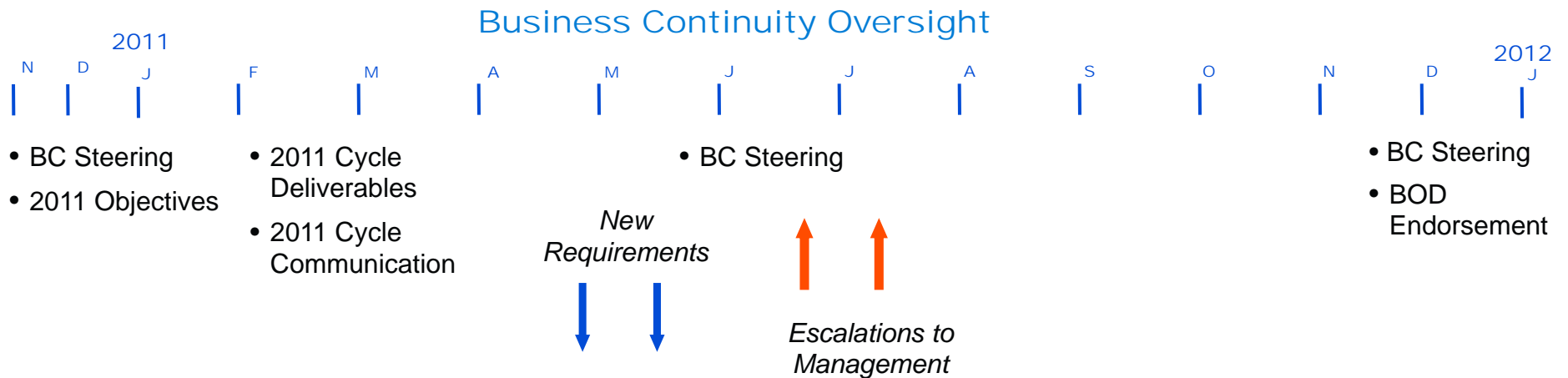
Disaster Recovery Strategy



Disaster Recovery Planning Cycle

Deliverables	Tier 1	Tier 2-3	Start Date	End Date
System Impact Analysis (BIA) Review (Tier 1, 2 & 3)	Y	Y	1-Mar	31-Jul
BIA Sign-off by Tech Owner and Business Owner	Y	Y	1-Mar	31-Jul
Plan Roster Review/Update (Quarterly)	Y	Y	Jan, Apr, Jul, Oct	
Recovery Plan Reviews	Y	Y	1-Apr	31-Oct
Technical Recovery Manual Review/Update	Y	Y	1-Sept	31-Oct
Team Activation Exercise	Y	Y	1-Apr	30-Sep
Plan Walkthrough Exercise	Y	Y	1-Apr	30-Sep
Disaster Recovery Exercise (Tier 1)	Y	N/A	Primary DC: Jun /Sep Secondary DC: May/Aug Secondary DC: Jul/ Oct Remote DC: Aug Remote DC: July	

Business Continuity Cycle - Full Timeline



Discussion Point - Planning

Have you established an effective BC/DR planning process?

- Enterprise-wide? Is management engaged? Is it ingrained in organizational culture?
- Who has ownership? What is BCMs role?
- How often do you test/exercise your BC/DR plan? How do you conduct test/exercise?
- Do you have a software planning tool? Who owns and administers the tool?
- How do you evaluate and measure the BC/DR plan ?

Have you ever executed the EM/CM, BC or DR plans? What were lessons learned?

Are BC and DR planning process integrated into a coordinated recovery of the business?

What are the issues or questions you have regarding BC/DR planning?

BCM Testing and Exercises

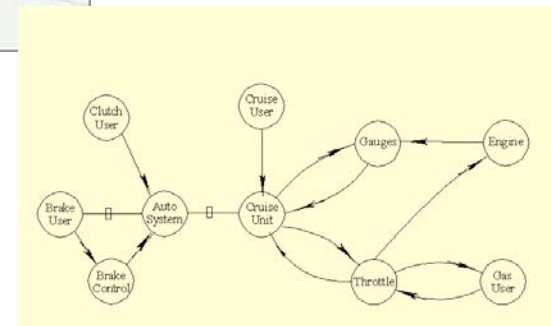


✓ Validates

- Plans
- Environment
- Data
- Operations

✓ Integrates

- Plans & Strategies
- Systems & Data
- Business Operations
- Customers
- 3rd Parties



Tests and Exercises

EM/CM Tests and Exercises

IAT Notification Test

IAT Tabletop Exercise - Self Conducted

CIRT/LIRT Notification Test

LIRT Scenario Based Exercise - Self Conducted

CIRT/LIRT Scenario Based Functional Exercise

BC Tests and Exercises

Work From Home Validation (Ess only)

Team Activation Exercise (Ess/Def)

Plan Walkthrough Exercise (Ess/Def)

Business Recovery Site Exercise (Ess only)

DR Tests and Exercises

Team Activation Exercise

Plan Walkthrough Exercise

Disaster Recovery Exercise (Tier 1)

BCM Testing and Exercises



✓ **Measures
Readiness**

✓ **Enhances and
Matures Plans**

✓ **Train**

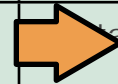
✓ **Educate**




✓ **Practice**



Exercise Ratings

#	Evaluation Criteria	Pts	Comments
1	Recovery strategies and times are defined	1	
2	Hardware and equipment capacities are adequate	1	
3	Network support and circuit capacities are adequate	0.5	Unable to validate network connectivity
4	Programs and operating procedures are established	1	
5	Data backup strategy is implemented	1	<p>Criteria:</p> <ul style="list-style-type: none"> • Recovery data identified • Data backed up • Data restoration meets RPO <p>Capabilities:</p> <ul style="list-style-type: none"> • Data backup in place • Back up data exercised <p>Limitations:</p> <ul style="list-style-type: none"> • Data was older than RPO <p>Score:</p> <ul style="list-style-type: none"> • Score of .05
6	Data recovery strategy provides data file recovery	0.5	
7	Support applications are available	1	
8	Recovery procedures are documented	1	
9	Communications procedures are documented	1	
10	Recovery team personnel are trained	1	
Final Score		9	



	Below Expectations	< 6.0
	Partially Meets Expectations	≥ 6.0 to < 8.0
	Meets Expectations	≥ 8.0

1	Recovery capabilities implemented to meet the criteria.
0.5	Recovery capabilities partially implemented to meet the criteria.
0	Recovery capabilities do not meet the criteria.



Exercise Ratings and Evaluations

Area	Exercise Performance	Recovery Readiness
Function A	9	10
Function B	10	10
Function C	10	10
Function D	10	10
System 1	9.5	9.5
System 2	8	8.5
System 3	9.5	9
Recovery Env.	<u>10</u>	<u>8.5</u>
	76	75.5

Overall Score: $76/8 = 9.5$
Superior Goal: 9.5

$75.5/8 = 9.43$

Year 2 Score: $72/8 = 9.0$

$72/8 = 9.0$

Year 1 Score: $69.5/8 = 8.69$

$66/8 = 8.25$

Measurements Based on BCM Cycles

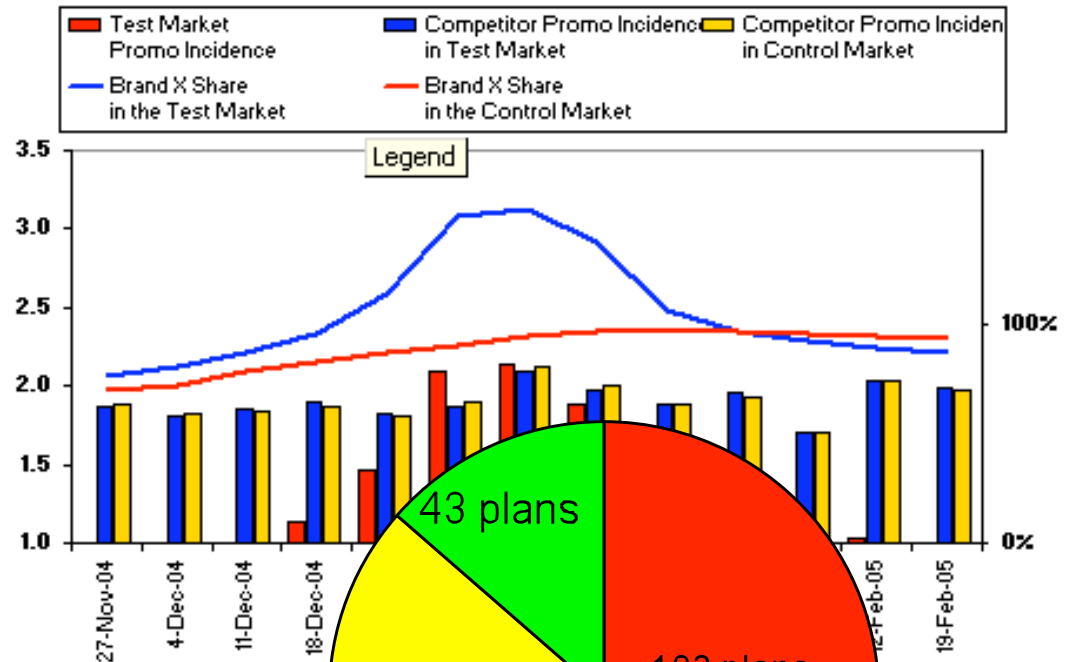
Deliverables	Core	Key	Small	Check	Measure
Business Impact Analysis (BIA) Review	Y	Y	Y	x	Updated BIA (date)
BIA Sign-off by Business Owner	Y	Y	Y	x	Sign-off by Business Owner
Plan Review/Update	Y	Y	N/A	x	Updated Plans (dates)
Business Continuity Manual Review/Update	N/A	Y	Y	x	Updated Manuals (dates)
Plan Roster Review/Update	Y	Y	Y	x	Updated Rosters (dates)
Work From Home Validation	Y	Y	Y	x	Survey and Sign-off
Team Activation Exercise	Y	Y	Y	x	Survey and Sign-off
Plan Walkthrough Exercise	Y	Y	N/A	x	Survey and Sign-off
Business Recovery Site Exercise	Y	N/A	N/A	x	Sign-in sheet, exercise checklist, survey

- Checklist measurement - manageable
- Validates completion of tasks and deliverables
- Lacks quality measurement

BCM Metrics



Share and Incidence for Test & Control Markets



✓ Gain commitment

✓ Show readiness

✓ Meet compliance

Measure BCM to demonstrate readiness

- Below Expectations < 6.0
- Partially Meets Expectations ≥ 6.0 to < 8.0
- Meets Expectations ≥ 8.0



Maintenance Processes and Cycles

Valuable corporate information



Maintenance Budget - Period 1					
Budget Object	Description	Fiscal Year 2000	Fiscal Year 2001	Fiscal Year 2002	Fiscal Year 2003
101	General Admin	10,000,000	10,000,000	10,000,000	10,000,000
102	Admin Support	5,000,000	5,000,000	5,000,000	5,000,000
103	Facilities	3,000,000	3,000,000	3,000,000	3,000,000
104	Information Systems	2,000,000	2,000,000	2,000,000	2,000,000
105	Legal & Compliance	1,000,000	1,000,000	1,000,000	1,000,000
106	Marketing	1,000,000	1,000,000	1,000,000	1,000,000
107	Operations	1,000,000	1,000,000	1,000,000	1,000,000
108	Personnel	1,000,000	1,000,000	1,000,000	1,000,000
109	Procurement	1,000,000	1,000,000	1,000,000	1,000,000
110	Research & Development	1,000,000	1,000,000	1,000,000	1,000,000
111	Security	1,000,000	1,000,000	1,000,000	1,000,000
112	Training	1,000,000	1,000,000	1,000,000	1,000,000
113	Travel	1,000,000	1,000,000	1,000,000	1,000,000
114	Utilities	1,000,000	1,000,000	1,000,000	1,000,000
115	Warranty	1,000,000	1,000,000	1,000,000	1,000,000
116	Other	1,000,000	1,000,000	1,000,000	1,000,000
117	Grand Total	100,000,000	100,000,000	100,000,000	100,000,000

Maintenance Budget - Period 2					
Budget Object	Description	Fiscal Year 2000	Fiscal Year 2001	Fiscal Year 2002	Fiscal Year 2003
101	General Admin	10,000,000	10,000,000	10,000,000	10,000,000
102	Admin Support	5,000,000	5,000,000	5,000,000	5,000,000
103	Facilities	3,000,000	3,000,000	3,000,000	3,000,000
104	Information Systems	2,000,000	2,000,000	2,000,000	2,000,000
105	Legal & Compliance	1,000,000	1,000,000	1,000,000	1,000,000
106	Marketing	1,000,000	1,000,000	1,000,000	1,000,000
107	Operations	1,000,000	1,000,000	1,000,000	1,000,000
108	Personnel	1,000,000	1,000,000	1,000,000	1,000,000
109	Procurement	1,000,000	1,000,000	1,000,000	1,000,000
110	Research & Development	1,000,000	1,000,000	1,000,000	1,000,000
111	Security	1,000,000	1,000,000	1,000,000	1,000,000
112	Training	1,000,000	1,000,000	1,000,000	1,000,000
113	Travel	1,000,000	1,000,000	1,000,000	1,000,000
114	Utilities	1,000,000	1,000,000	1,000,000	1,000,000
115	Warranty	1,000,000	1,000,000	1,000,000	1,000,000
116	Other	1,000,000	1,000,000	1,000,000	1,000,000
117	Grand Total	100,000,000	100,000,000	100,000,000	100,000,000



- ✓ Establish Schedule
- ✓ Define responsibilities

- ✓ Reliable information
- ✓ Dynamic
- ✓ Significant Volume of Data

- ✓ Automate
- ✓ Reuse data - single source
- ✓ Develop Streamline Processes

What data is maintained by Users vs. BCM?

Discussion Point - Validate & Metrics

Do you have an effective BCM exercise/testing process?

- What level of testing is performed and what areas are tested? Is the organization committed?
- How are tests/exercises conducted for CM/EM, BC and DR? What is the frequency?
- Who has exercise/testing ownership? What is BCMs role?
- What are the issues or questions you have regarding exercise/testing process

What are the issues or questions you have regarding testing/exercise process?

Do you have an evaluation, rating and reporting process for BCM?

- How do you measure the exercise/tests?
- How do you evaluate and rate plans (EM/CM, BC, DR)?
- Who is responsible for evaluating and rating plans?
- How are ratings maintained and stored? How do you report results to management?
- Does the evaluation, rating and reporting process drive the BCM Program?

What are the issues or questions you have regarding evaluation, rating and reporting?

What are your maintenance processes and practices?



Randall J. Till, MBCP

Till Continuity Group

314-608-7672

randall@tillcontinuity.com

