Taking a Proactive Approach to Crisis Management while Maintaining Business Continuity in a Tiered Environment

John Linse
Director of Business Continuity Services, EMC

Setting the Stage

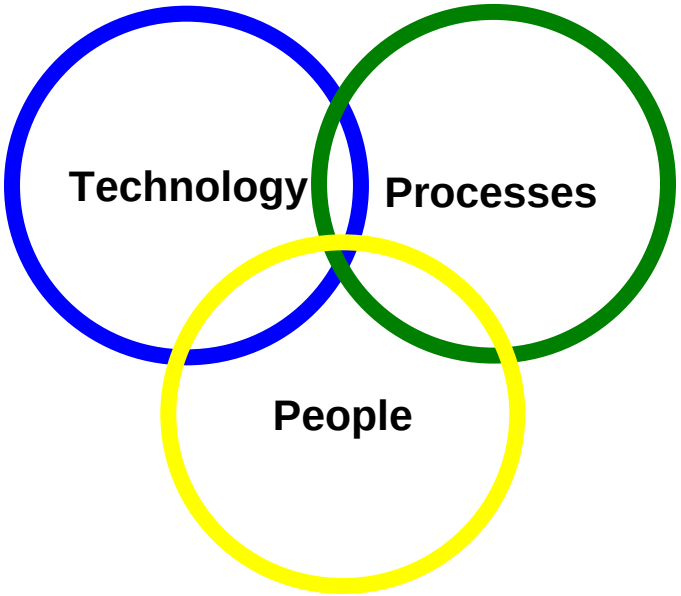
Taking a Proactive Approach to Crisis Management while Maintaining Business Continuity in a Tiered Environment

- Defining Business Continuity
- Developing a Tiered Environment
- Managing a Crisis

Defining Business Continuity

Assuring that Business process continue in the face of an event that causes employees to leave their normal work environment and conduct business in an unusual manner

- Key elements of a Business Continuity Program
  - Technology – Disaster Recovery
  - Business Process management
  - People Skills
- Disaster Recovery Should be a Service
  - Recovery Objectives Defines
  - Recovery Procedures Tested
- People Should understand Their Role
  - Who Declares a Disaster
  - How is the “Drill” Managed
- Business Processes need to be prioritized
  - Key information flows
  - Understanding Supporting Resources

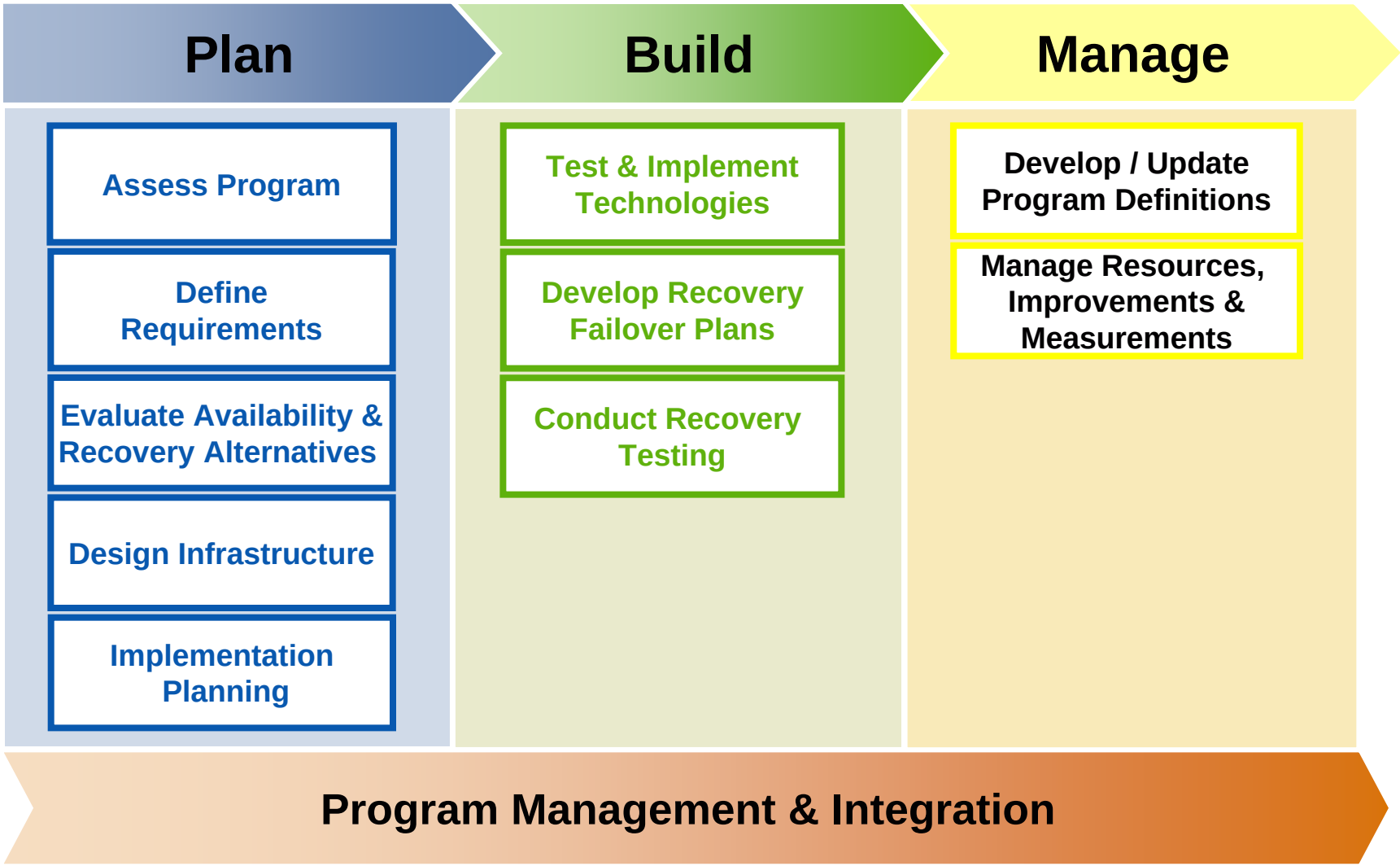


Developing a Tiered Environment

Business Processes and Applications should be prioritized by their impact to the Business in the case of an Event. Their Recovery Objectives need to match the investment that the Business will make based upon the impact of an outage.

- Understanding Impact
  - Who defines it
  - How is Remediation Maintained
- Not all Applications or Processes are Created Equal
  - Recovery objectives are equal to Impact
  - Less Important Processes have a lower Priority
  - Plans should stratify the severity of an Event
- Tiered Environments include:
  - Technology across all aspects of the “Stack”
  - Defined Business Requirements
  - Associated Reference Architectures
  - Supporting Processes
  - Operational (Acquisition) Cost Model

Developing a Tiered Environment



Developing a Tiered Environment

Characteristic
Application attributes that need to be defined to align to service tiers

Specifications
Metric that application attributes need to be defined in to align to defined tiers

Tier Metrics
Service level attributes supported by IT and offered to customers

- **Archiving (AR)** Inactive (policy based) application data storage services
- **Operational Recovery (OR)** Application data version storage services for recovery of data in case of a catastrophic server / application failure or data corruption / deletion
- **Disaster Recovery (DR)** Application data version storage services for recovery of systems / data in case of a catastrophic data center failure

	Alignment Scheme	Alignment Specification	Tier 1	Tier 2	Tier 3	Tier 4
Primary Storage	Guaranteed Performance	Performance Throughput Per Port (I/O sec)	5,000+	up to 5,000	up to 3,500	up to 1,500
		Response Time (ms)	< 8ms	7-14ms	12-30ms	22-30ms
	Availability	Maximum Unplanned Downtime Per Year (Min)	< 26.5	< 26.5	< 52.5	< 263
	Cost	$/Usable GB	$111	$65	$33	$22
Archiving Storage	Performance	Response Time	< 1 Second	< 1 Second	< 24 Hours	
		Throughput	<= 300 Mbps	<= 700 Mbps	<= 280 Mbps	
	Availability	Downtime (Yr)	< 5.25 Min	< 52.56 Min	< 175.2 Hr	
	Retention & Disposition	Retention Period	< 30 Years	< 10 Years	< 3 Years	
		Data Shredding Compliance	Yes	No	No	
	Accessibility	Read / Annual Access Frequency	< Hourly	< Hourly	Daily	
	Data Integrity	Guarantee of Authenticity	Yes	No	No	
	Off-Site	Recovery Point Objective	<1 Minute	<28 Hours	<38 Hours	
	Cost	$/Usable GB	$35	$25	$11	
Operational Recovery	Recovery Classification	Recovery Classification	Complete Application Restore	Complete Application Restore	File or File System Restore	File or File System Restore
	Operational Recovery Point Objective	Amount of Data Loss	1 Hour	24 Hours	24 Hours	30 days
	Operational Recovery Time Objective	Time Required For Recovery	< 30 Minutes	< 30 Minutes	7 GB/Min	.5 GB/Min
	Recoverability	Ability To Recover Backed Up Data	100%	100%	98%	95%
	Retention Period	Length of Time That Data Is Retained	2 Hours	24 Hours	3 Weeks	15 months
	Cost	$/Usable GB	$46 - $13	$44- $13	$8	$5
Disaster Recovery	Disaster Recovery Point Objective (RPO)	Amount Of Data Loss	0 Minutes	< 4 Hours	24 - 48 Hours	24 - 48 Hours
	Disaster Recovery Time Objective (RTO)	Time Required To Restore Data	< 2 Hours	< 12 Hours	< 48 Hours	< 72 Hours

Reference Architecture by Service Attribute

Defined Recovery Requirement by Service Attribute

Ownership and Operation Financial Model

Prioritized of Service Characteristics to Align Application

Managing a Crisis

….And all the Kings Horses and all the Kings Men couldn't put him back together again….

- Have a Plan for Crisis Management, Communications, and Disaster Recovery
  - Identify Roles and Responsibilities
  - Identify Prioritized Activities, and Interdependencies
  - Establish and Manage your command post
- Stratify your planning to respond to the severity of the event
  - Application Outages
  - Temporary Denial to Workspace Without Damage
  - Temporary Denial to Workspace with Damage
  - Long Term Denial to Workspace
- You can plan for the response of an event, but you can’t always plan on the event itself.
- Know your Chain of Command
  - Know who can declare a disaster
  - Know who manages the program
  - Have a Plan B; Be sure to have an Accountability Plan

Managing a Crisis

….And all the Kings Horses and all the Kings Men couldn't put him back together again….

- Remember Human Interest
  - People will put their family and personal interests before their company
- Test you plan
  - Disaster Drills – with defined objectives
- Establish you Business Continuity Program Office
  - Have a Charter
  - Define your Initiatives
  - Define the Companies Key Performance Indicators
  - Define the Audit Policies and Process
- Business Continuity is about
  - Cultural Change
  - Risk Mitigation

Thank You

John S. Linse
Director Business Continuity Services
EMC
Linse_John@EMC.com