

## 2013 DIR Telecommunications Forum

---

# Disaster Recovery: What You Should (already) Know

27 June 2013



**Bob Smock, CISSP, CISM, PMP**  
Senior Director  
Security and Risk Management  
Gartner Consulting  
[bob.smock@gartner.com](mailto:bob.smock@gartner.com)

### GARTNER

DIR Telecommunications Forum

Version #1

This presentation, including any supporting materials, is owned by Gartner, Inc. and/or its affiliates and is for the sole use of the intended Gartner audience or other authorized recipients. This presentation may contain information that is confidential, proprietary or otherwise legally protected, and it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.  
© 2012 Gartner, Inc. and/or its affiliates. All rights reserved.

**Gartner**

## Disaster Recovery: What You Should Know Bad Things Do (and Can) Happen

---

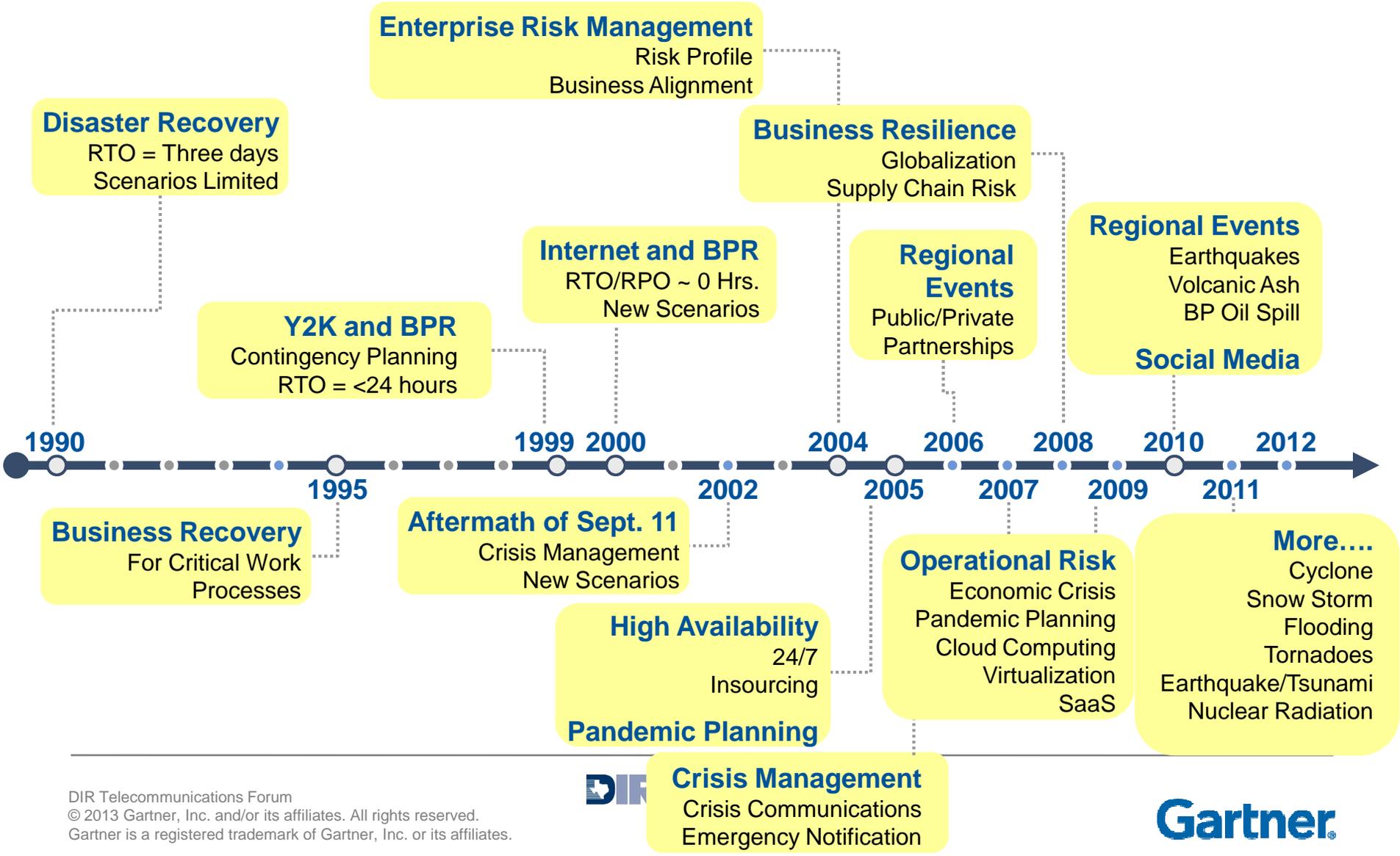
- Bastrop Fires
- Super-storm Sandy
- Hurricane Ike
- Japan Earthquake/Tsunami
- Tornado Alley
- Acts of Terrorism/Civil Unrest
- Cyber attacks
- Airport incidents/Nuclear fallout
- North Korean Missiles (maybe)
- Avian Flu/Pandemic workforce outage
- Zombie Apocalypse



Note: BCM = business continuity management; RCO = recovery time objective; RPO = recovery point objective; SaaS = software as a service.

# Business Continuity Evolution

## From Disaster Recovery to Business *Resiliency*



## Disaster Recovery: What You Should Know Texas Government Trends

- Good News: 80% of agencies have established disaster recovery and business continuity plans
- Bad News: More than 70% of agencies:
  - Do not perform regular and periodic reviews of the plans to ensure changes in the business or technological environments have been appropriately addressed
  - Do not have comprehensive plans that cover all assets required to fulfill the mission of the agency
  - Have not tested the plans within the last three years



*Leaving open the question as to whether the plans provide adequate capabilities for timely restoration and maintenance of services provided by the agency during an unexpected outage*

## Disaster Recovery: What You Should Know Solving the Problem

2. A 3-kg object is released from rest at a height of 5m on a curved frictionless ramp. At the foot of the ramp is a spring of force constant  $k = 100 \text{ N/m}$ . The object slides down the ramp and into the spring, compressing it a distance  $x$  before coming to rest.

10 (a) Find  $x$ .  
5 (b) Does the object continue to move after it comes to rest? If yes, how high will it go up the slope before it comes to rest?

$U = 3(9.8)(5) = 147.15$   
 $U_s = \frac{1}{2}(100)x^2 = 50x^2 \dots?$

**No. there is an elephant in the way.**

# Disaster Recovery: What You Should Know

## DR Modernization: Because Business – and Life – Happens on IT



**Supply Chain**

**Government Resiliency**

**e-Commerce**



**Banking**

**Finance**

**Healthcare**

## Disaster Recovery: What You Should Know

### Key Recovery Trends

---

1. **Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) have dropped significantly** because dependency on business systems has increased, with the business costs of downtime escalating across all industries.
  2. Organizations are opting for a **layered strategy for tiered recovery** to contain costs, matching the quality of service to the criticality of the IT service.
  3. Enterprises are implementing a **more granular application or business system recovery** approach, as opposed to complete site failover.
  4. The implementation of recovery SLAs or targets is driving more systematic analysis and implementation of an architecture that **matches appropriate recovery solutions to the criticality of business systems**.
  5. **Tape is being used for recovery of last resort** and for long-term retention (archiving).
- 

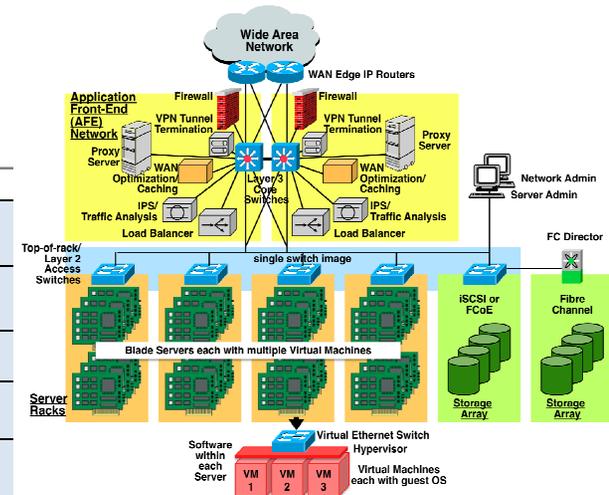


(C) TheLightningMan.com

# Disaster Recovery: What You Should Know

## Scope of the Problem: Availability Checklist

➔	<b>COMPREHENSIVE DISASTER RECOVERY Strategy &amp; PLAN</b>
	<b>PERIODIC REIEW &amp; UPDATE OF DR PLAN</b>
	<b>PERIODIC TESTING OF PLAN &amp; Training of Participants</b>
➔	<b>CONTINUITY OF OPERATIONS PLAN SUPPORTED BY DR PLAN</b>
➔	<b>Pandemic/long-term remote access plan and capabilities</b>
	<b>BUSINESS IMPACT ANALYSIS</b>
	<b>BIA VETTED WITH BUSINESS PROCESS/APPLICATION OWNERS</b>
➔	<b>DR PLAN WITH RTO &amp; RPO ESTABLISHED AND REALISTIC BASED ON BIA</b>
	<b>Use of STATE OF THE ART MEDIA AND TECHNIQUES</b>
	<b>STRATEGY including DAILY, WEEKLY, MONTHLY, QUARTERLY, ANNUAL</b>
	<b>BACKUPS CONTAIN DATA, APP SOURCE CODE, SYSTEM IMAGES</b>
	<b>DATA ITEM RECOVERY FROM BACKUPS HAS BEEN TESTED</b>
	<b>Full system/service restoration from backups has been tested</b>
➔	<b>Alternate Data Center strategy</b>
	<b>Data Center alternate long-term power (generator)</b>
	<b>OFF SITE STORAGE FOR BACKUPS</b>
★	<b>ENCRYPTION (OR OTHER PROTECTION) FOR BACKUP MEDIA THAT CONTAINS SENSITIVE DATA</b>



## Disaster Recovery: What You Should Know

### Scope of the Problem: Restoration Complexity

$$D = \frac{1}{c} \frac{dL}{dt} = \frac{1}{cP} \frac{dP}{dt}$$

$$D^2 = \frac{1}{P^2} \frac{P_0 - P}{P} \sim \frac{1}{P^2} \quad (1a)$$

$$D^2 = \frac{K_0}{3} \frac{P_0 - P}{P} \sim \frac{1}{K_0} \quad (2a)$$

$$D^2 \sim 10^{-53}$$

... and then a miracle happens ...

$$\begin{aligned} P &\sim 10^0 \text{ } \{ \text{L, J} \\ \tau &\sim 10^{10} (10^{11}) \} \end{aligned}$$

- ☑ All required data center equipment installed and operational?
- ☑ Which files are databases & which are restored 1st, 2nd, 3rd, ...?
- ☑ Which application startup procedures are run first, second, third, ...?
- ☑ For application X, which transactions need to be tested and why?
- ☑ What evidence (run books, log files, handwritten notes) needs to be collected and retained?

\*Based on 24/365 or 8760 hours/year scheduled uptime

Disaster Recovery: What You Should Know  
 Today's Always-On World Increases Expectations

*Benchmarking Availability: Hours Down/Year/IT Service*

	<b>Unplanned</b>	<b>Planned</b>
<b>Very Good</b>	Fewer than 61.32 hours (99.3%)*	Fewer than 200 hours
<b>Outstanding</b>	Fewer than 26.28 hours (99.7%)*	Fewer than 50 hours
<b>Best in Class</b>	Fewer than 4.38 hours (99.95%)*	Fewer than 12 hours
<b>Continuous Availability</b>	Zero (100%)	Zero (100%)

**Typical Mission Critical**

**2-3%**

*End-to-End Application Availability*

**Example Only**

Disaster Recovery: What You Should Know  
 Strategy: Criticality Levels Based on BIA and **Cost of Downtime**

Criticality Level	Business Processes	Scheduled Uptime	Avail. %	RTO	RPO
Mission-Critical	External — constituent communications, revenue	24/7	99.95 22 min/mo	15 min	0
Critical	Internal — ERP, email	24 hrs/day, 6.5 days/wk, 12 hrs/year for upgrades	99.9 41 min/mo	4 hrs	4 hrs
Important	Internal — financial systems	24/6	99.5 3 hrs/mo	48 hrs	24 hrs
Noncritical	Internal — departmental systems, experimentation	24/5	98	1 week	24 hrs

**Example Only**

# Disaster Recovery: What You Should Know

## Strategy Architecting for Availability: Planned & Repeatable

	Gold	Silver	Best Effort
SLAs	Continuous Availability	99.5, RTO=4 hours	98, RTO = 48 hours
Cost	9*X	4*X	X
Architecture	Active/Active/Hot	Active/Passive/Warm	Active/Cold
Infrastructure Requirements	<ul style="list-style-type: none"> <li>• Full redundancy/capacity</li> <li>• "Hot-plug" hardware</li> <li>• Use of GA and vendor-supported products</li> <li>• Spare parts on-site</li> </ul>	<ul style="list-style-type: none"> <li>• Redundant architecture</li> <li>• Shared resources 2nd site</li> <li>• Manually initiated failover</li> <li>• Vendor MTRS SLA</li> </ul>	<ul style="list-style-type: none"> <li>• Stand-alone servers</li> <li>• Autorestart</li> <li>• Tested backup</li> <li>• No SPOF — user NW</li> </ul>
Software and Development Requirements	<ul style="list-style-type: none"> <li>• Autorecovery</li> <li>• No transaction loss</li> <li>• User resp. time monitoring</li> <li>• Test environment = production environment</li> </ul>	<ul style="list-style-type: none"> <li>• App design failover</li> <li>• Autodiagnostics</li> <li>• Scalable</li> <li>• Secure</li> </ul>	<ul style="list-style-type: none"> <li>• Application start/stop</li> <li>• Tested recovery plan</li> <li>• Change management</li> </ul>
Operational Requirements	<ul style="list-style-type: none"> <li>• Real-time alarming with business impact</li> <li>• Capacity planning</li> <li>• Outage prevention</li> <li>• Managed staged upgrades with parallel failback</li> </ul>	<ul style="list-style-type: none"> <li>• Proactive tuning</li> <li>• Proactive A&amp;P mgmt.</li> <li>• Proactive problem management/RCA</li> <li>• Biannual DR tests</li> <li>• Tested rollback plans</li> </ul>	<ul style="list-style-type: none"> <li>• Change management</li> <li>• Event monitoring</li> <li>• Backup practices</li> <li>• Well-trained staff</li> <li>• Tested recovery plan</li> </ul>

### Architectural Standards for Infrastructure, Software, & Operations

**Example Only**

# Disaster Recovery: What You Should Know

## Map Application Groups to Service Levels and Strategy

### Application Group A

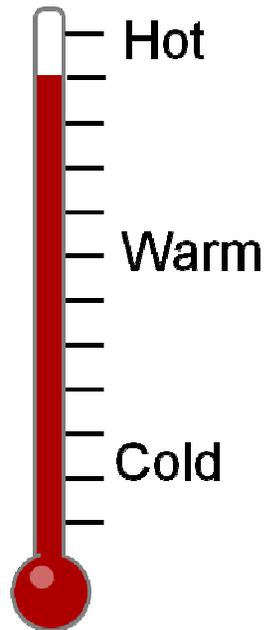
Scenario	RTO	RPO	Retention	Example Strategy
Local or remote recovery (corruption)	4 hours	4 hours	24 hours	Snapshot and CDP or log-based roll-forward
Local recovery (user error)	1 day	4 hours	1 week	Snapshot, Oracle Flashback, individual mailbox recovery, etc.
Change causing downtime	8 hours	Point before change made	N/A	Snapshot before change and recover locally, or failover to disaster recovery site where change not yet made
Site disaster	1 hour	0 hours	N/A	Continuous sync. replication
Multiple point of failure	1 hour	0 hours	N/A	Same as above; failover entire application group
Sabotage or last resort	1 day	24+ hours	60-90 days	Tape-based backup

*Map Scenario with Required Service Levels to Appropriate Strategy*

# Disaster Recovery: What You Should Know

## Everything Comes With a Cost

How hot is hot enough?

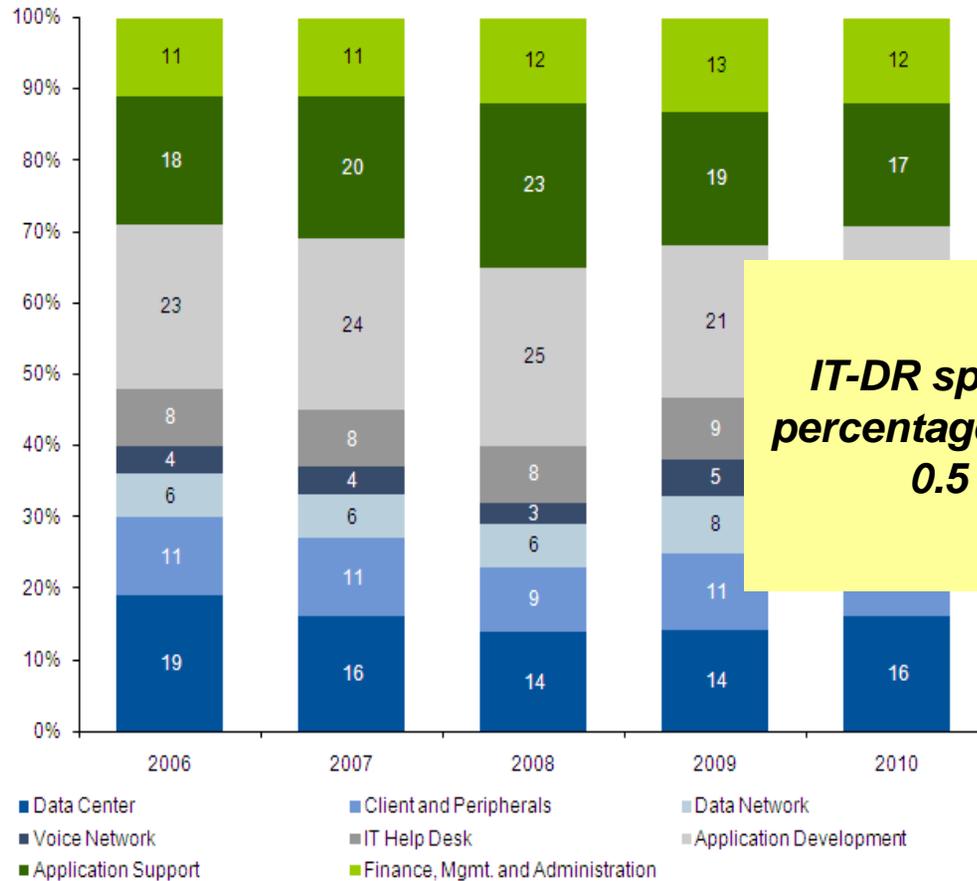


How much are you willing to pay for it?

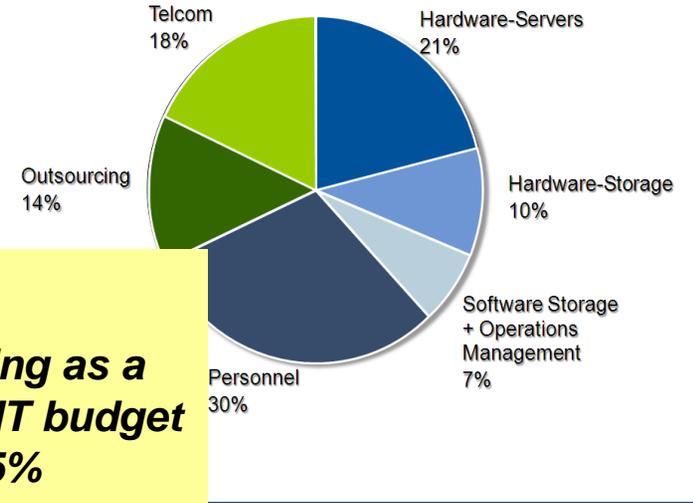
RTO	Solution Architecture	Relative Cost
0-seconds	Active/Active or Active/Passive/Auto-Failover	\$\$\$\$
1 hour	Active/Passive (save up to 50% on software licensing)	\$\$\$
4+ hours	Active/Passive/Shared (save up to 50% on shared hardware)	\$\$

# Disaster Recovery: What You Should Know

## IT DR and Data Center-specific Spending



**IT-DR spending as a percentage of IT budget 0.5 – 2.5%**



	Weighted DR Spending Percentage	Relative Year-to-Year Increase
2009	4.2%	---
2010	4.9%	16.7%
2011	4.6%	-6.1%

Source: 2011 Gartner Security and Risk Management Survey (N=165)

**Data Center Spending = 16% of IT budget**

# Disaster Recovery: What You Should Know

## IT Recovery Time Targets and IT Budget Spend by Vertical

	<b>Vertical Industry</b>	<b>RTO &amp; RPO Requirements</b>	
1	<b>Airlines – Reservations and Booking Systems</b> <b>Communications – Telecom</b> <b>Financial Services – Depository Institutions</b> <b>Financial Services – Other</b>	<b>Vertical Industry Group I</b> <b>(0 - 2 hour RTO,</b> <b>0 - 2 hour RPO)</b>	<b>DR Spending:</b> <b>5.x% to 8%</b> <b>(or more)</b> <b>of IT Budget</b>
2			
3			
4			
5	<b>Biotechnology</b> <b>Defense</b> <b>Financial Services – Insurance</b> <b>Government – Federal</b> <b>Healthcare – Hospitals/Healthcare Providers</b> <b>Information Technology</b> <b>Manufacturing – Discrete – All</b> <b>Manufacturing – Process – All</b> <b>Media</b> <b>Pharmaceutical</b> <b>Services – Professional</b> <b>Utilities</b>	<b>Vertical Industry Group II</b> <b>(2 hours - 8 hours RTO,</b> <b>2 hours - 4 hours RPO)</b>	<b>DR Spending:</b> <b>3.x% to 5%</b> <b>of IT Budget</b>
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17	<b>Consumer Goods</b> <b>Distribution – Retail</b> <b>Education</b> <b>Government – State and Local</b> <b>Petroleum</b> <b>Transportation (except for airlines)</b>	<b>Vertical Industry Group III</b> <b>(8 Hours - 24 hour RTO,</b> <b>4-24 hour RPO)</b>	<b>DR Spending:</b> <b>1.x% to 3%</b> <b>of IT Budget</b>
18			
19			
20			
21			
22			
23	<b>Construction</b> <b>Distribution – Wholesale</b> <b>Food &amp; Beverage</b> <b>Hospitality</b> <b>Non-Profit</b> <b>Publishing</b>	<b>Vertical Industry Group IV</b> <b>(More than 24 hours RTO,</b> <b>More than 24 hours RPO)</b>	<b>DR Spending:</b> <b>.5% to 1%</b> <b>of IT Budget</b>
24			
25			
26			
27			
28			

# Disaster Recovery: What You Should Know

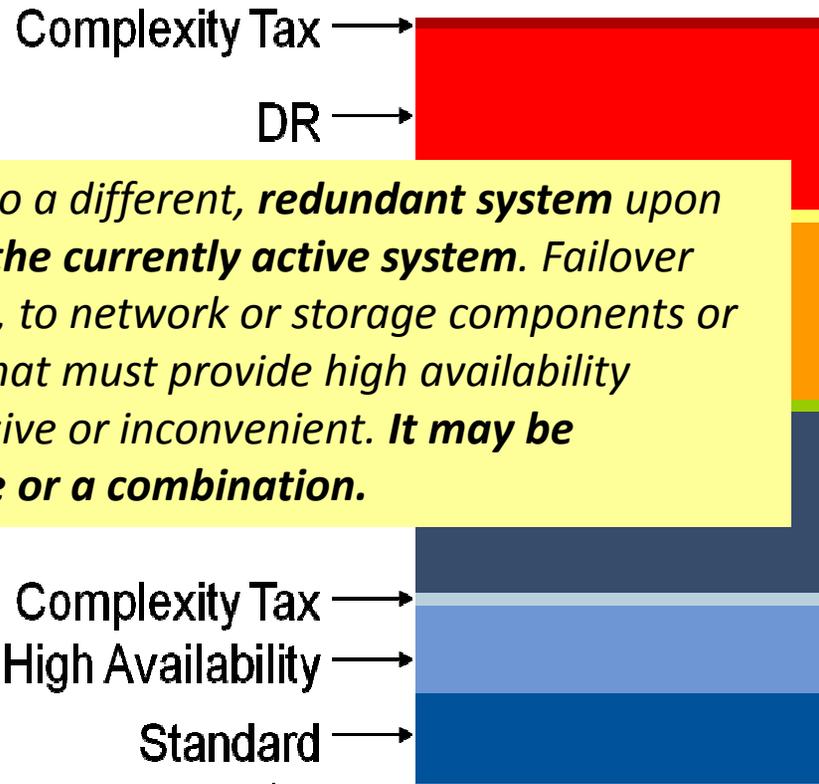
## Recovery Data Center Strategies



### Considerations

- Considerations:
  - Cost
  - Distance
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Complexity
  - Production/Dev-Test-DR
  - Production Load Sharing

### High Availability



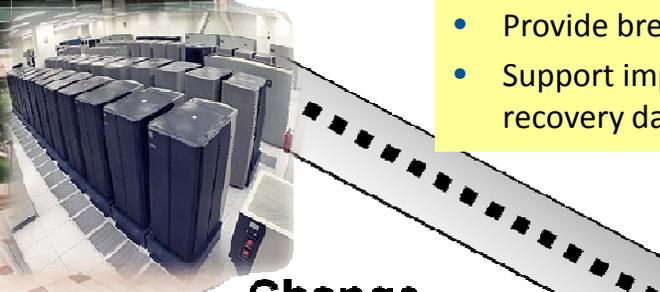
**Failover** -- Automatically switching to a different, redundant system upon failure or abnormal termination of the currently active system. Failover can be applied to a cluster of servers, to network or storage components or any other set of redundant devices that must provide high availability because down-time would be expensive or inconvenient. **It may be implemented in hardware, software or a combination.**

## How Many Data Centers?

# Disaster Recovery: What You Should Know

## Change Management Challenges

### Production Data Center



**Change  
Synchronization**

#### Needed: Procedures and/or software that:

- Detect configuration changes in primary and recovery configurations
- Reconcile against configuration policy
- Reconcile or matches changes to approved change requests
- Remediate incorrect configuration changes
- Prevent unauthorized configuration changes
- Manage workflow for configuration release changes
- Provide breadth and depth of data center infrastructure support
- Support improved configuration consistency between primary and recovery data centers



**Backup Data Center**

# Disaster Recovery: What You Should Know

## Lots of Ways to Eat the Elephant

	DR Service Providers	In-sourced Management	Colo/Hosting Providers	Recovery-in-the-Cloud Providers
Cold Site	○	N/O	●	N/O
Warm Site	○	●	●	◐
Hot Site	○	●	●	◐
Shared Data Center Equipment	○	N/O	◐	◐
Dedicated Data Center Equipment	○	●		N/O
Data Replication and Restoration	○	●	◐	◐
Virtual Machine Backup & Restoration	○		◐	◐
IT Equipment Drop Ship	○		N/O	N/O
Mobile Data Center Recovery	○	●	N/O	N/O
Mobile Workarea Recovery	○	●	N/O	N/O
DR Test Management	◐	●	●	◐

Hybrid Solutions

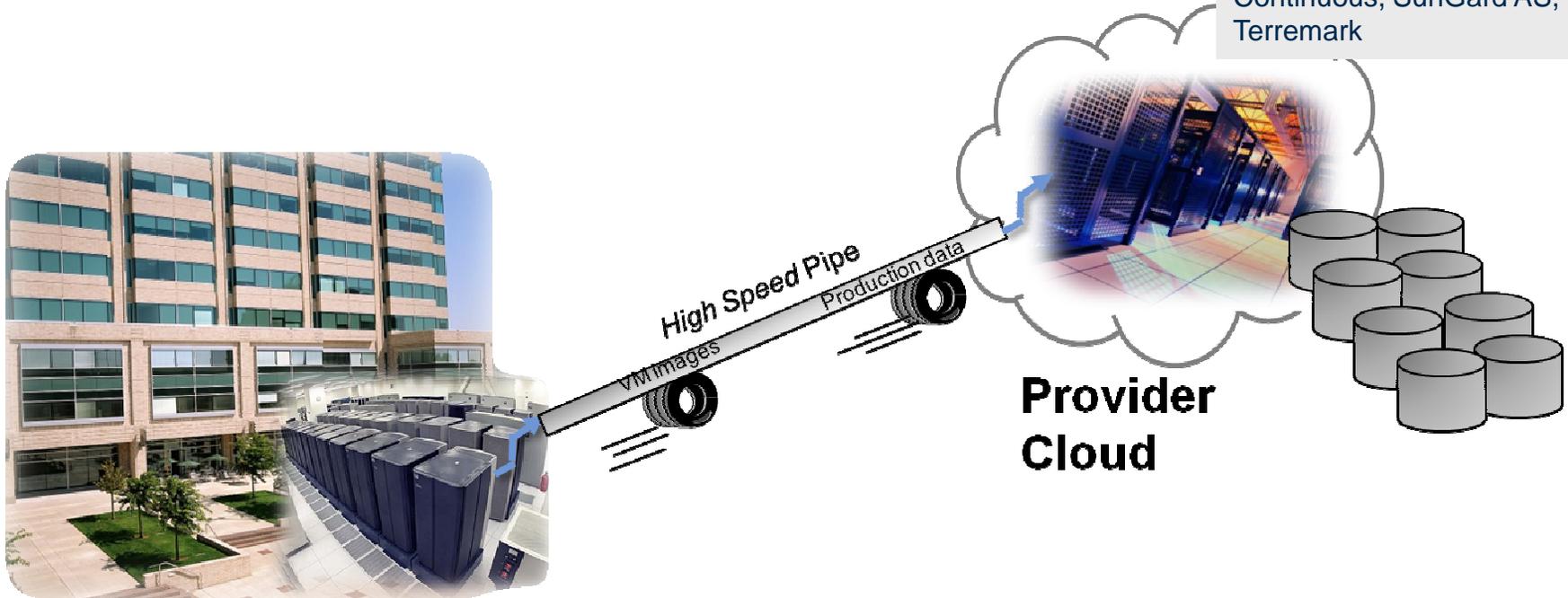
○ Provider Responsibility    ◐ Varies by Provider    ● IT Responsibility    ◑ Shared Responsibility    N/O Service not offered

*How much do you need to own in order to hit recovery & availability targets?*

# Disaster Recovery: What You Should Know

## Recovery-in-the-Cloud

- Offered by \* :  
Allstream, Amazon, AT&T, Bluelock, Doyenz, Geminare, Hosting.com, i365, iland, IPR International, Navisite, Qwest, Rackspace, Savvis, Simply Continuous, SunGard AS, Terremark



**Enterprise Data Center**

\* - North America only

*Managed replication of VMs and production data into the provider cloud  
Production systems may either be in the enterprise or at the service provider site*

# Disaster Recovery: What You Should Know

## Service Subscription Model

Service Provider	Provider Customer
<ul style="list-style-type: none"> <li><input type="checkbox"/> Provides facility floor space</li> <li><input type="checkbox"/> <u>Provisions equipment for Testing</u> <ul style="list-style-type: none"> <li><input type="checkbox"/> Mainframes</li> <li><input type="checkbox"/> Legacy systems</li> <li><input type="checkbox"/> Servers</li> <li><input type="checkbox"/> Storage</li> <li><input type="checkbox"/> Network connectivity</li> <li><input type="checkbox"/> Desktop devices (if needed)</li> <li><input type="checkbox"/> On-site hands (optional)</li> </ul> </li> <li><input type="checkbox"/> Blocks of test time (in days)</li> <li><input type="checkbox"/> <u>Charges:</u> <ul style="list-style-type: none"> <li><input type="checkbox"/> Between \$1.5K and \$5K+ per month (varies by recovery configuration)</li> <li><input type="checkbox"/> Fee for disaster declaration</li> <li><input type="checkbox"/> Daily usage fee (if applicable)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Typically commits to a three or five year contract</li> <li><input type="checkbox"/> Pays monthly fee(s) to provider</li> <li><input type="checkbox"/> Provides dedicated space for testing and recovery operations</li> <li><input type="checkbox"/> Responsible for equipment costs</li> <li><input type="checkbox"/> Typically responsible for installing production applications and staging production data</li> <li><input type="checkbox"/> Performs test exercise(s)</li> <li><input type="checkbox"/> Refines test orchestration in order to ensure that key RTOs and RPOs can be met</li> <li><input type="checkbox"/> Repeats above steps annually</li> </ul>

Remember: You can't delegate risk

## Disaster Recovery: What You Should Know

### New or Renewal DR Service Investment Decision Criteria

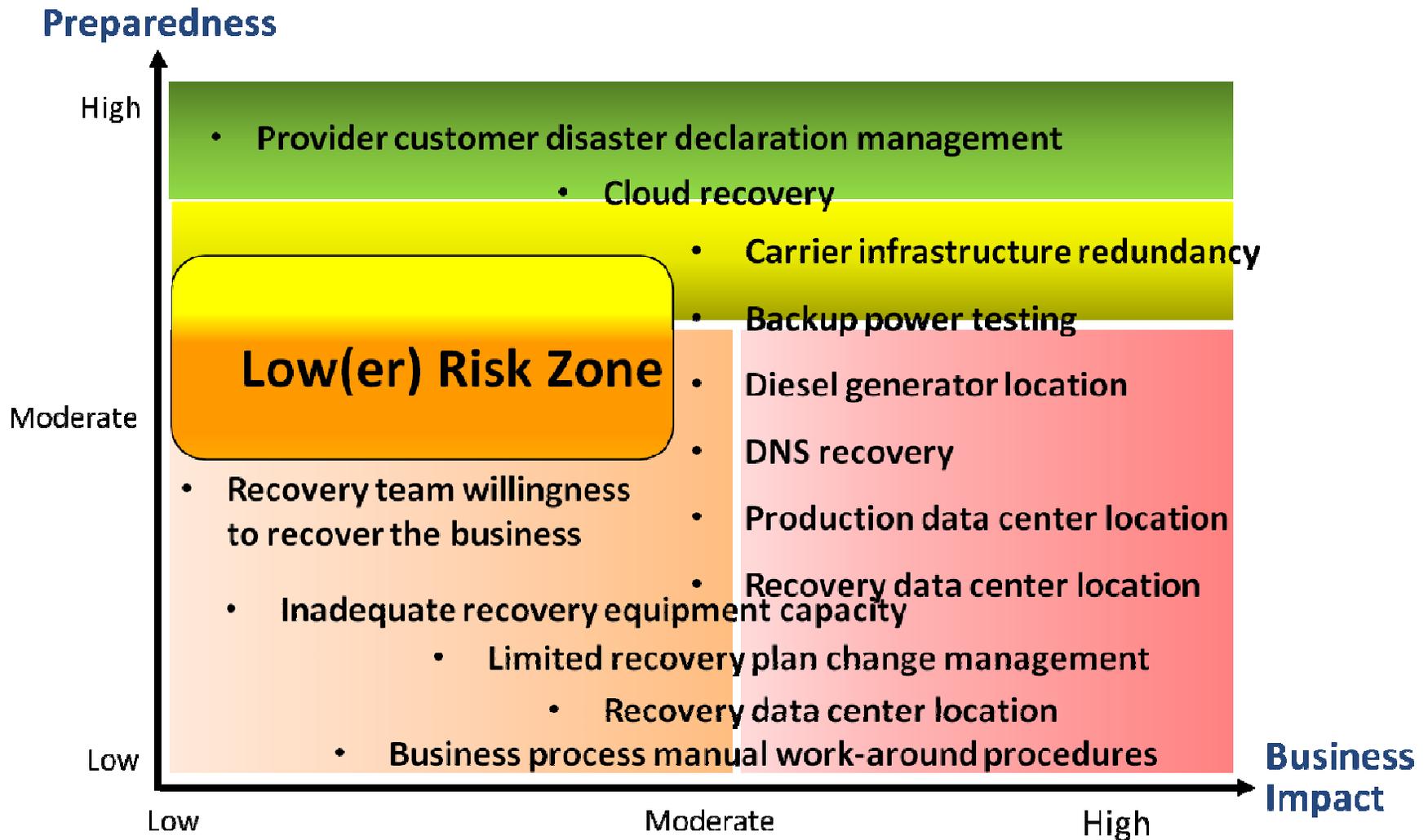
---

- Computing platform support
  - z-Series, i-Series, p-Series, Solaris, HP-UX, Windows, Linux
- Incremental facilities costs
  - Own space
  - DR provider
  - Colocation/hosting
  - Cloud
- Dedicated versus shared equipment
- RTO and RPO service Levels
- Self-serve versus managed configuration setup
- Self-serve versus managed testing
- \$\$\$ per month per managed terabyte of storage
- Physical and logical network costs and limitations
- Applications failover and failback management
- Responsibility for tape-based backup and recovery



# Disaster Recovery: What You Should Know

## Data Center Operations Impact Heat Map



## Disaster Recovery: What You Should Know

### Data Center Operations: Lessons Learned

---

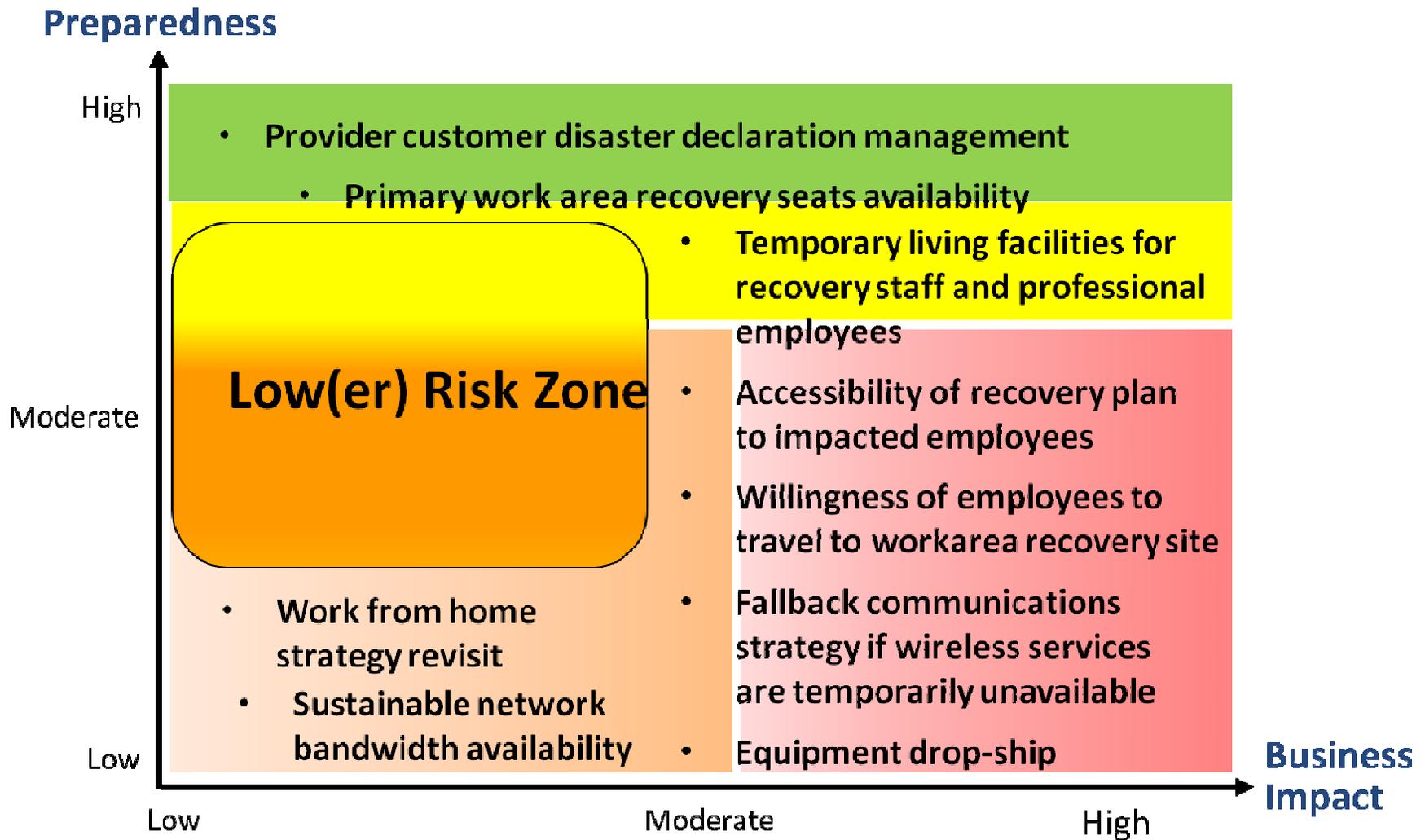
- ✓ More due diligence required for determining carrier services availability risk
- ✓ The recovery team that you *think* you have and the recovery team that you *actually* have may be very different
- ✓ Need to do a better job in determining compute and storage resource requirements, *especially* if extended recovery operations are required
- ✓ Re-set needed regarding recovery data center location (as well as the primary production data center location)
- ✓ Scope expansion needed for manual business process workarounds
- ✓ Have all the production apps been recovery tested within the past two years?
- ✓ More frequent testing needed for backup power (UPS and generator)
- ✓ Logical network services (for example, DNS) *must* be highly available



Lessons  
Learned

# Disaster Recovery: What You Should Know

## Work Area Recovery Impact Heat Map



## Disaster Recovery: What You Should Know

### Work Area Recovery: Lessons Learned

---

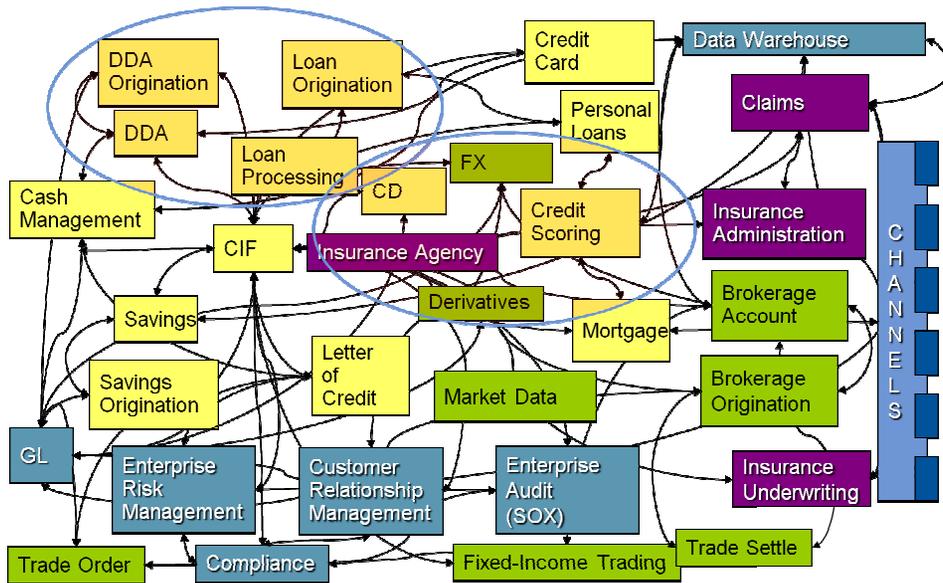


Lessons  
Learned

- ✓ When performing recovery facility due diligence, need to assess both number of available recovery seats *and* hotel capacity in the surrounding area.
- ✓ Maintain awareness of critical employees' willingness to travel to a remote work area recovery site.
- ✓ Ensure that all employees have an externally accessible recovery plan and a simple cheat sheet (for example, a laminated card) that explains critical recovery steps and how to access sources of updated information.
- ✓ Check your drop ship equipment provider's contingency plans for delivering critical recovery equipment.
- ✓ Evaluate the feasibility of providing key employees with alternative communications mechanisms (for example, satellite phones) if mainstream mobile phone and network services are temporarily unavailable.
- ✓ Need to ensure that a full set of manual or semi-manual work-around procedures for critical business processes are both in-place and tested

# Disaster Recovery: What You Should Know

## Next Steps: The Approach



- ✓ Identify integration points and dependencies
- ✓ Plan data synchronization
- ✓ Link application groupings with RTO and RPO
- ✓ Develop exception scenarios
- ✓ Prepare failover granularity and grouping

*Develop a Recovery Plan for [Complex] IT Environments*

# Disaster Recovery: What You Should Know

## Next Steps: Assess

### Impacts

- ❌ Reduced ability to maintain knowledge, skills, procedures, and technologies sufficient to provide adequate and appropriate recovery from disasters in support of the enterprise business continuity plan for continuing services at necessary levels
- ❌ Reduced confidence that existing plan, will provide adequate or appropriate guidance in enabling the enterprise to recover from disasters in support of the enterprise business continuity plan for continuing services at necessary levels
- ❌ Reduced confidence in the enterprise business continuity plan and the capability to provide appropriate level of recovery commensurate with established service recovery objectives
- ❌ Resources, effort, and funding may not be commensurate with the recovery requirements of specific applications potentially resulting in either an over-spend scenario or a weakened business continuity posture

### Approach

- ✅ Develop and vet an enterprise Business Impact Analysis (BIA) with realistic Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) commensurate with assurance-level of each application and aligned with service recovery objectives established in enterprise Business Continuity Plan (BCP)
- ✅ Conduct an assessment of enterprise disaster recovery requirements as established in the enterprise business continuity and disaster recovery plans. Use results of the assessment to establish a formal, comprehensive disaster recovery strategy and supporting architecture including appropriate technology, processes and staffing
  - ❑ Ensure recovery strategy includes sufficient alternate processing and remote access capabilities to support extended primary outages commensurate with criticality and assurance requirements

*Know the Targets and Constraints*

# Disaster Recovery: What You Should Know

## Next Steps: The Plan

### Impacts

- ❌ Reduced ability to maintain knowledge, skills, procedures, and technologies sufficient to provide adequate and appropriate recovery from disasters in support of the enterprise business continuity plan for continuing services at necessary levels
- ❌ Reduced confidence that existing plan, will provide adequate or appropriate guidance in enabling the enterprise to recover from disasters in support of the enterprise business continuity plan for continuing services at necessary levels
- ❌ Reduced confidence in the enterprise business continuity plan and the capability to provide appropriate level of recovery commensurate with established service recovery objectives
- ❌ Resources, effort, and funding may not be commensurate with the recovery requirements of specific applications potentially resulting in either an over-spend scenario or a weakened business continuity posture

### Approach

- ✅ Develop a formal, comprehensive disaster recovery planning process that includes regular and periodic reviews, management and stakeholder approval, & integration with business contingency and enterprise planning processes
  - ❑ Maintain and enhance the plan through regular and periodic formal testing of partial and full recovery capabilities for all
  - ❑ Recovery capabilities should be based on objectives determined through business impact assessment and established in enterprise business continuity plan
  - ❑ Coordinate plan review and update cycle with plan testing cycle
  - ❑ Reviews and tests should occur at least annually, with complete review and full, live-testing at least every 2 – 3 years

*Perform effective Planning & Testing*

## Questions and Answers

---

### Contacts

**Bob Smock, CISSP, CISM, PMP**  
Senior Director  
Security and Risk Management  
Gartner Consulting  
[bob.smock@gartner.com](mailto:bob.smock@gartner.com)



#### **GARTNER**

DIR Telecommunications Forum

Version #1

This presentation, including any supporting materials, is owned by Gartner, Inc. and/or its affiliates and is for the sole use of the intended Gartner audience or other authorized recipients. This presentation may contain information that is confidential, proprietary or otherwise legally protected, and it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.  
© 2012 Gartner, Inc. and/or its affiliates. All rights reserved.

