The ABC's of BCP

Jeremy Sucharski
Governance Risk and Compliance – G31

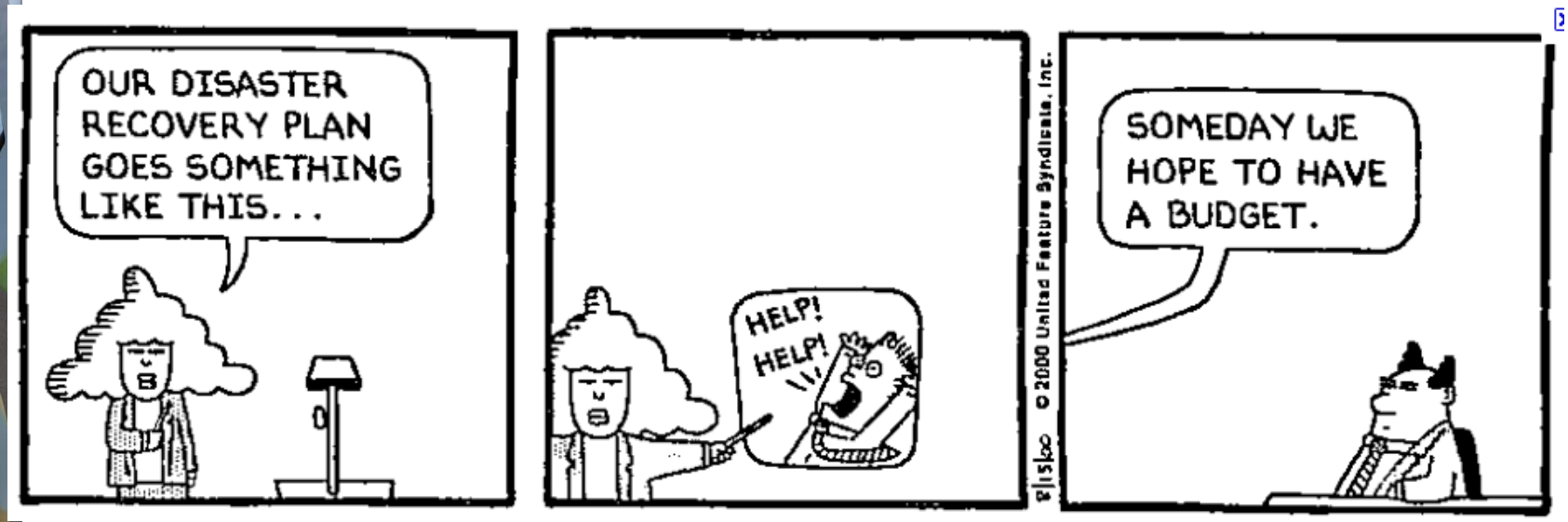
Jeremy Sucharski, CISA, CRISC

- Over 12 years of experience
- CISA and CRISC Certifications
- Governance, Risk and Compliance Practice Leader at Armanino McKenna
- Cal Poly SLO and Deloitte & Touché ERS Alumni
- Experience with:
  - SOX
  - SOC/SAS70
  - IT Audit Support
  - Information Security
  - Process Optimization
  - Contract Assurance
  - DR & BCP
- Have designed implemented, tested and audited DR and BCP plans for companies of varying sizes and industries.

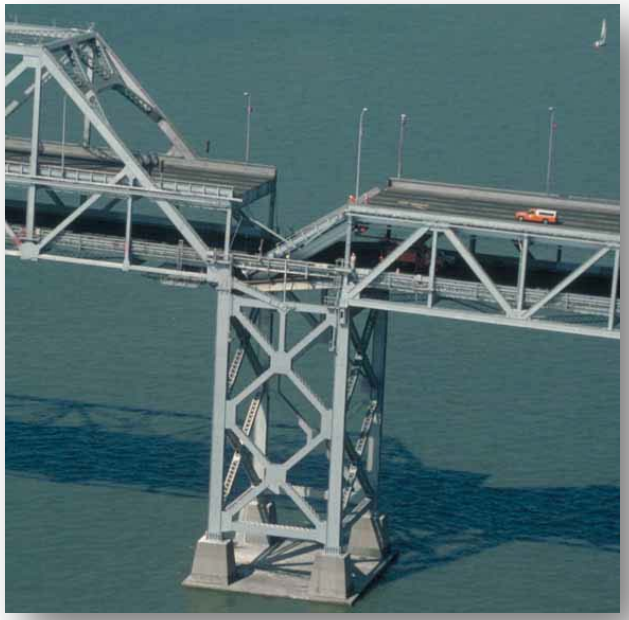
Session Topic Overview

- Business Continuity Statistics
- Dispelling BCP Fallacies
- Business Continuity Planning Process
- Steps for Success
- Audit Considerations
- Question and Answer Throughout

Dilbert's Wisdom



A Matter of Perspective



Which of these scenario's comes to mind when you hear "Business Continuity" or "Disaster Recovery"

Commonality?

= ?

Why are DR and BCP Important?

71%	• 71% of companies have some form of DR or Business resumption Plan
59%	• 59% of plans were updated in last year
82%	• 82% were tested in past year

Why are DR and BCP Important?

90%

- 90% of companies who cannot recover operations within 5 days go out of business s within 1 year

Why are DR and BCP Important?

- Top 3 Causes of Unplanned System Outages:
  - System Upgrades and Patching
  - Power Failure/Issue
  - Fire
- Average Cost of an Unplanned Outage:
  - $287,000

Business Continuity Fallacies

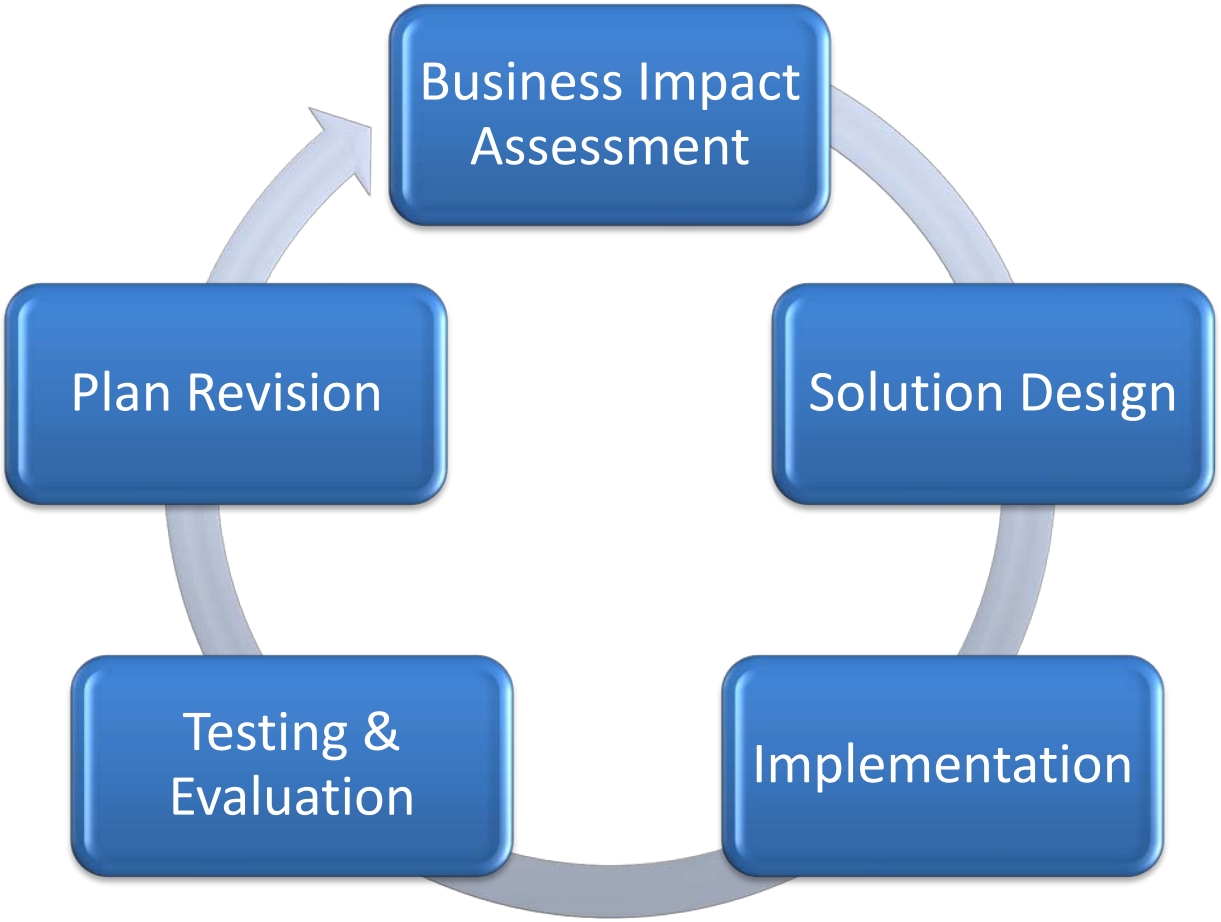
- One Time Event
- Executed in a Vacuum
- Only focused on IT Systems
- An absolute assurance
- Disaster Recovery Planning
- Focused only on large disasters

- An ongoing Process
- Part of the company culture
- Basis For *Reasonable* Assurance of recovery
- Process to mitigate risks
- Focused on Critical Processes

Alphabet Soup

- Key Acronyms to know before beginning the BCP Process
  - BCM
  - BCP
  - DR
  - RTO
  - RPO
  - MTPD

Components of Effective Business Continuity Planning



Planning Is Everything…

Business Impact Assessment Components

Data Gathering

Inventory

Analysis

Reporting

Data Gathering

- Begin by “defining” your organization
- Communicate process to entire company
- Identify key individuals to participate in the process
- Ensure that this includes a cross section of:
  - Job functions
  - Positions / Levels
  - Responsibilities

Data Gathering

- Develop a standard output for your interviews
  - Summary information
  - Dependent Applications
  - Related or Dependent Processes
  - Peak Periods/Seasonality
  - Loss Impact Analysis
  - Process Description
- Request supporting data throughout
- Leverage Data Gathering for educating company

Inventory

- Compile what you learned in your interviews and other data gathering
  - Hardware
  - Software
  - Processes
  - Locations
  - Owners
- “You cant analyze what you haven’t discussed.”

Analysis

- Leverage output from Data Gathering and Inventory Phases
- May include a wide variety of analysis categories including:

Downtime	Environmental	Loss Impact	Strategy
Peak Time	Data	Intellectual Property	Man Made Risk
Location	Contractual Obligation	Cyber Attack	Employee Sensitivity
RTO	RPO	Recovery Approach	Customer Relationships

Loss Impact Analysis

Loss Category	Weight	Score (1-5)	Weighted Average	Comments
Financial	68			
Reputation	10			
Client Service	10			
Operational Ability	10			
Safety	1			
Legal & Regulatory	1			

~Example Loss Impact Analysis Criteria Matrix~

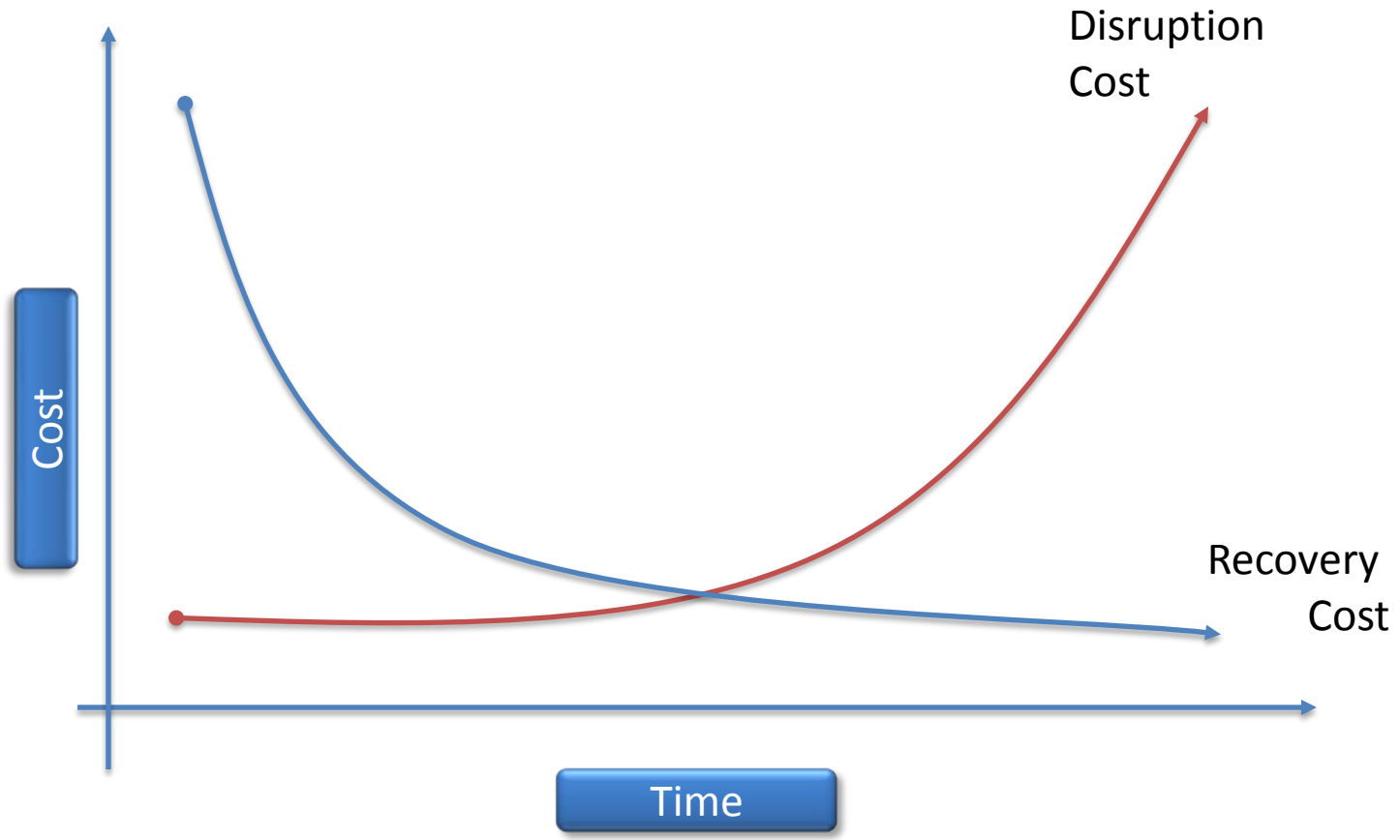
Reporting

- Audience
  - Executive
  - Managerial
- Format
  - Include formats that can be leveraged in Solution Design
    - e.g. tables of action items, etc.
- Frequency
  - Initial Reporting
  - Status Reporting

Reporting

Table of Contents

Solution Design Challenge



Solution Design

- Evaluate Recovery Strategies
  - Hot
  - Warm
  - Cold
  - Cloud
  - SaaS
  - Reciprocal agreements
  - Local
  - Geographically Separate
- Identify Primary and Recovery Locations
- Translate recovery requirements into actions for IT

Solution Design

- Identify alternative work locations
- Identify executive recovery location
- Evaluate business interruption insurance
- Evaluate recovery priority

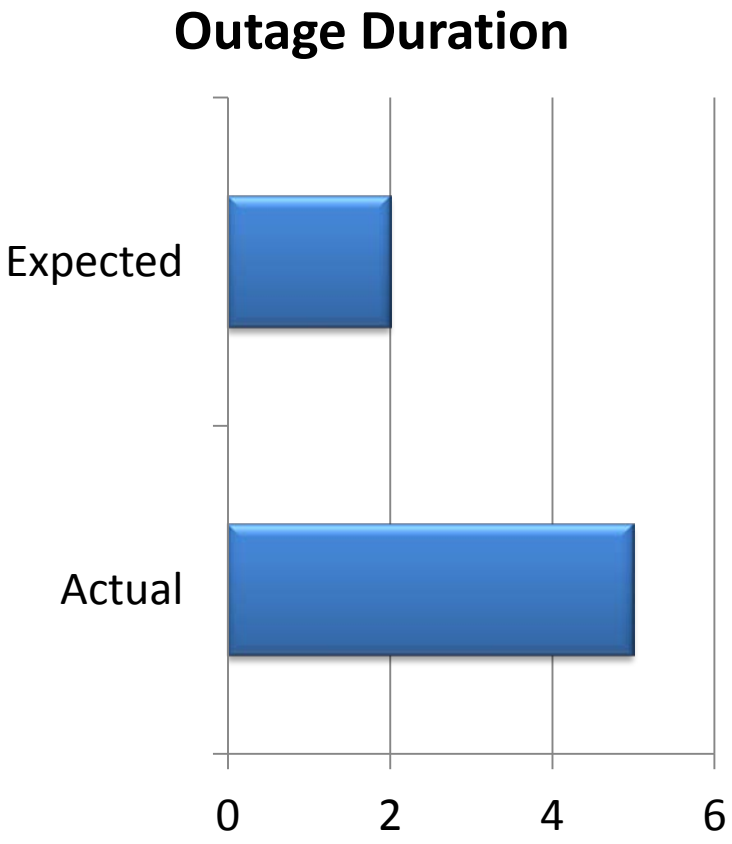
Solution Design

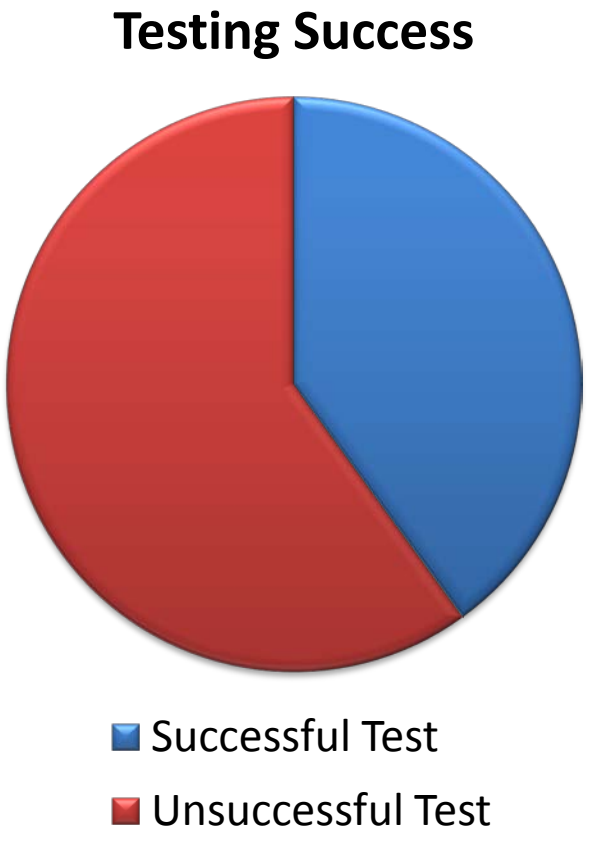
- Define recovery approach
- Form recovery team
- Document and Communicate Implementation Plan
- Fold into existing IT plans (if possible
- Leverage SME's
- Categorize Tasks/Effort:
  - Technology
  - Process
  - Training and Education

Solution Design

- Emergency communication process
- Emergency response procedures
- Emergency leave and pay policy
- Define departmental recovery plans

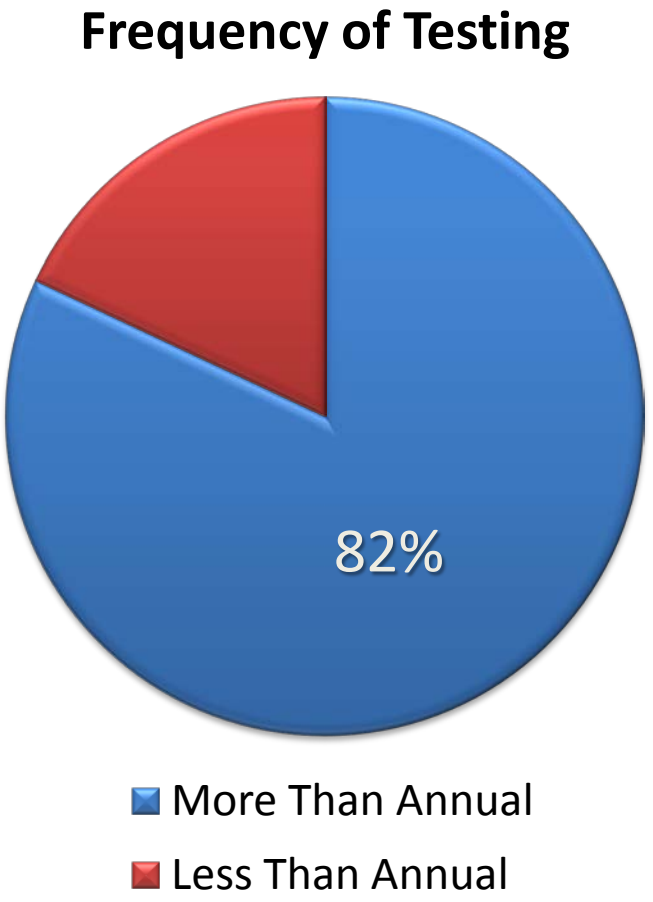
How Good Is Your Plan?





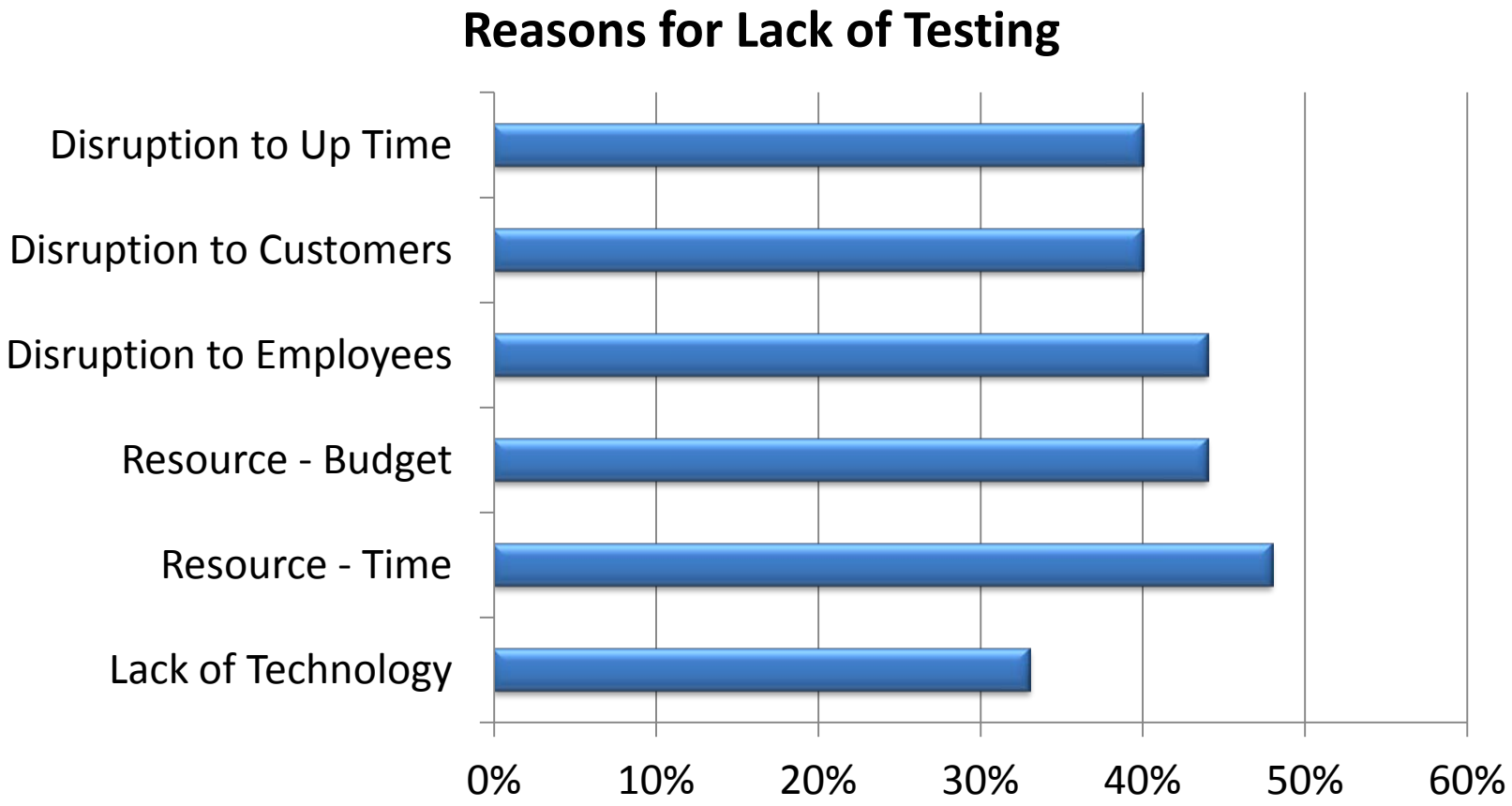
Testing & Improvement

- Test Your Plan
  - What % of companies test their DR or BCP plans more than annually?

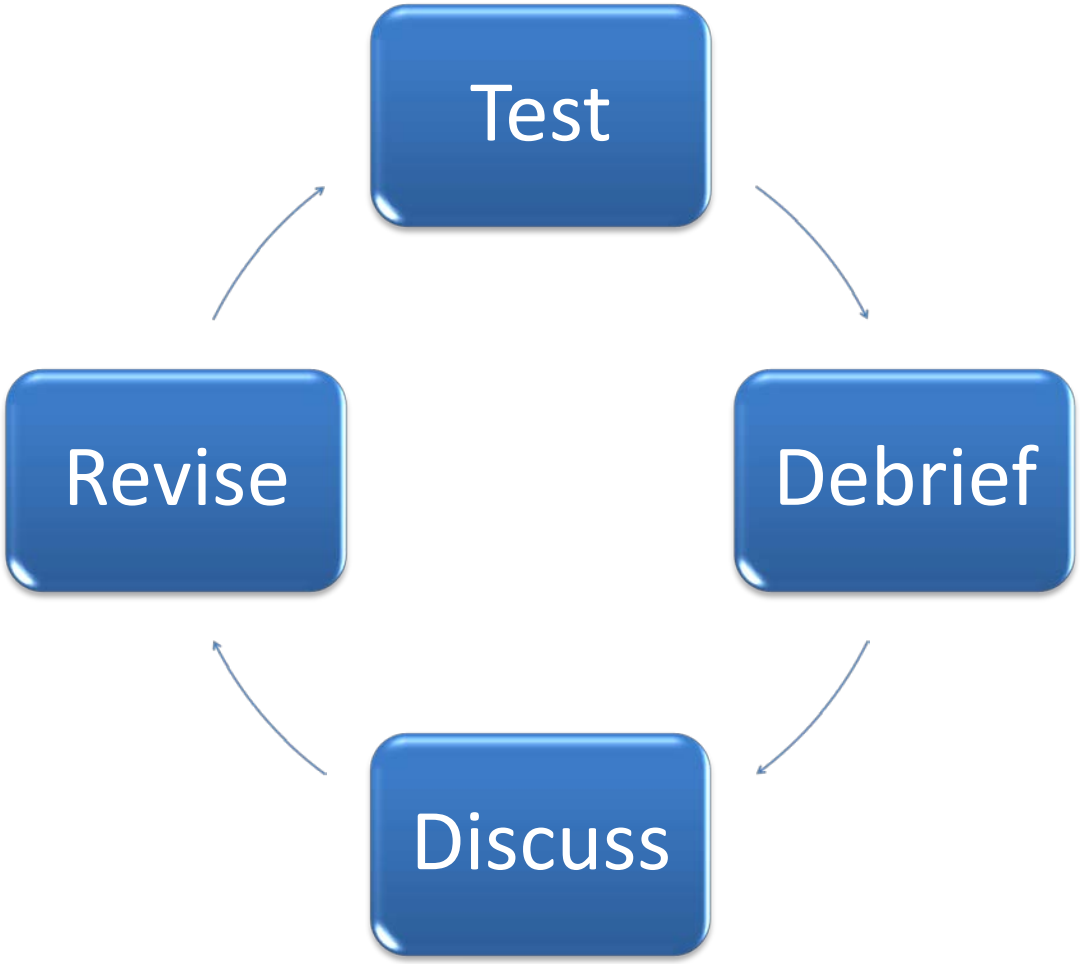


28

So Why Skip The Testing?



Testing & Improvement



Testing & Improvement

- Types of Testing:
  - Table Top Testing
  - Crisis command team call-out testing
  - Fail Over Testing
  - Technical swing test from primary to secondary work locations
  - Full Recovery Exercise

Trends

- BCM is #2 area of increased IT Spending
- Increased Focus at C-Suite
  - Driven by:
    - Strategy
    - Compliance
    - Business Environment
- Integrating BCP, ERM and Risk Assessment

Trends

- Virtualization
- Cloud
- Mobile
- Social Media
- Big Data
- ISO 22301

Audit Considerations

- BCM Team Organization and Communication
- Policy, Standards and Procedures
- BIA
- Risk Assessment
- Documentation and Distribution

Audit Considerations

- Testing
  - Frequency
  - Type
  - Results
- Maturity Assessment

What Questions Do You Have?