Business Continuity Planning, Including Cloud Hosting Considerations

Steve Shofner, Senior Manager,
Armanino LLP

Core Competencies – C23

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

SF ISACA FALL CONFERENCE NOVEMBER 9-11, 2015 HOTEL NIKKO-SAN FRANCISCO

Learning Objectives

During today's webinar, participants will:

- Identify the difference between Business Continuity Planning and Disaster Recovery Planning
- Describe steps companies can take to implement a Disaster Recovery plan
- Ensure successful deployment and maintenance of a Disaster Recovery plan

Presentation Overview

- Defining ‘Disasters’
- Why Plan?
- Planning Approach
  - Cloud Considerations
- Testing & Continuous Improvement
- Trends
- Audit Considerations

DEFINING DISASTERS

Defining Disasters

Sudden, calamitous event that brings great damage, loss or destruction.
(*Source: Merriam-Webster dictionary*)

Natural

- Earthquake
- Flood
- Hurricane
- Drought
- Twister
- Tsunami
- Cold/Heat wave
- Thunderstorm
- Mudslide

Man-Made

- Riots
- War
- Terrorism
- Power outages
- Sprinkler system bursts
- Equipment sabotage
- Arson
- Epidemic
- Pollution
- Transportation accident
- Food poisoning

Technological

- Database corruption
- Hacking
- Viruses
- Internet worms

“Disasters” Come in all sizes

Small

Large

WHY PLAN?

Top Causes and Effects

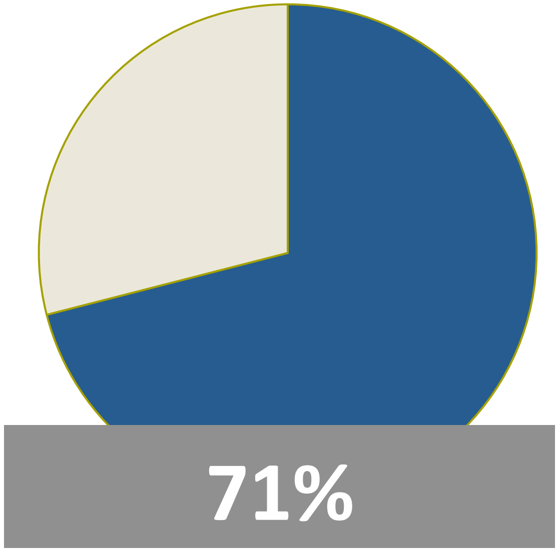
Top 3 Causes of Unplanned System Outages

1. System Upgrades and Patching
2. Power Failure/Issue
3. Fire

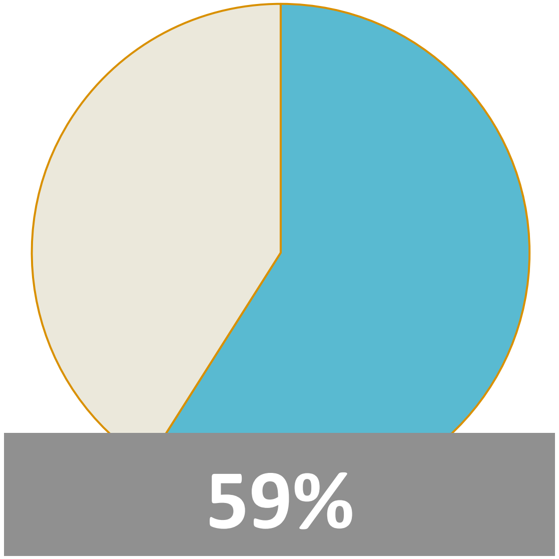
Drivers for Having a Business Continuity Plan (BCP)

- High availability of data is required by your industry
- Regulatory requirements
- Contractual obligation with a business partner
- It makes good business sense!

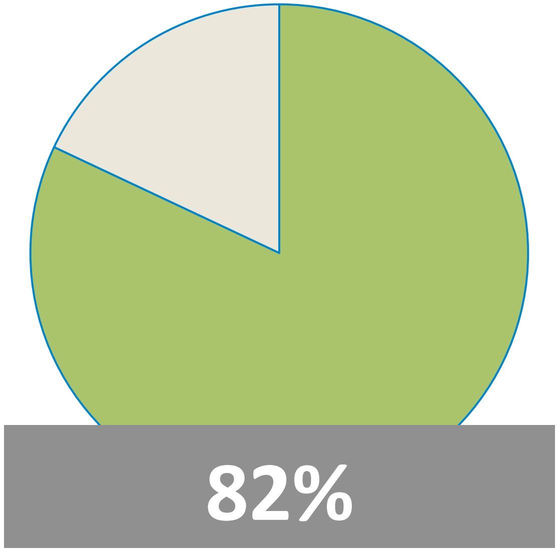
Some Statistics



Companies that have some form of DR or Business resumption Plan



Plans that were updated in last year



Plans that were tested in the last year

Why are DR and BCP Important?

90%

of companies that cannot recover operations within 5 days go out of business within 1 year

PLANNING APPROACH

Disaster Recovery Plans vs. Business Continuity Plans

Disaster Recovery Plans

Successfully recover IT systems in the shortest timeframe possible.

Business Continuity Plans

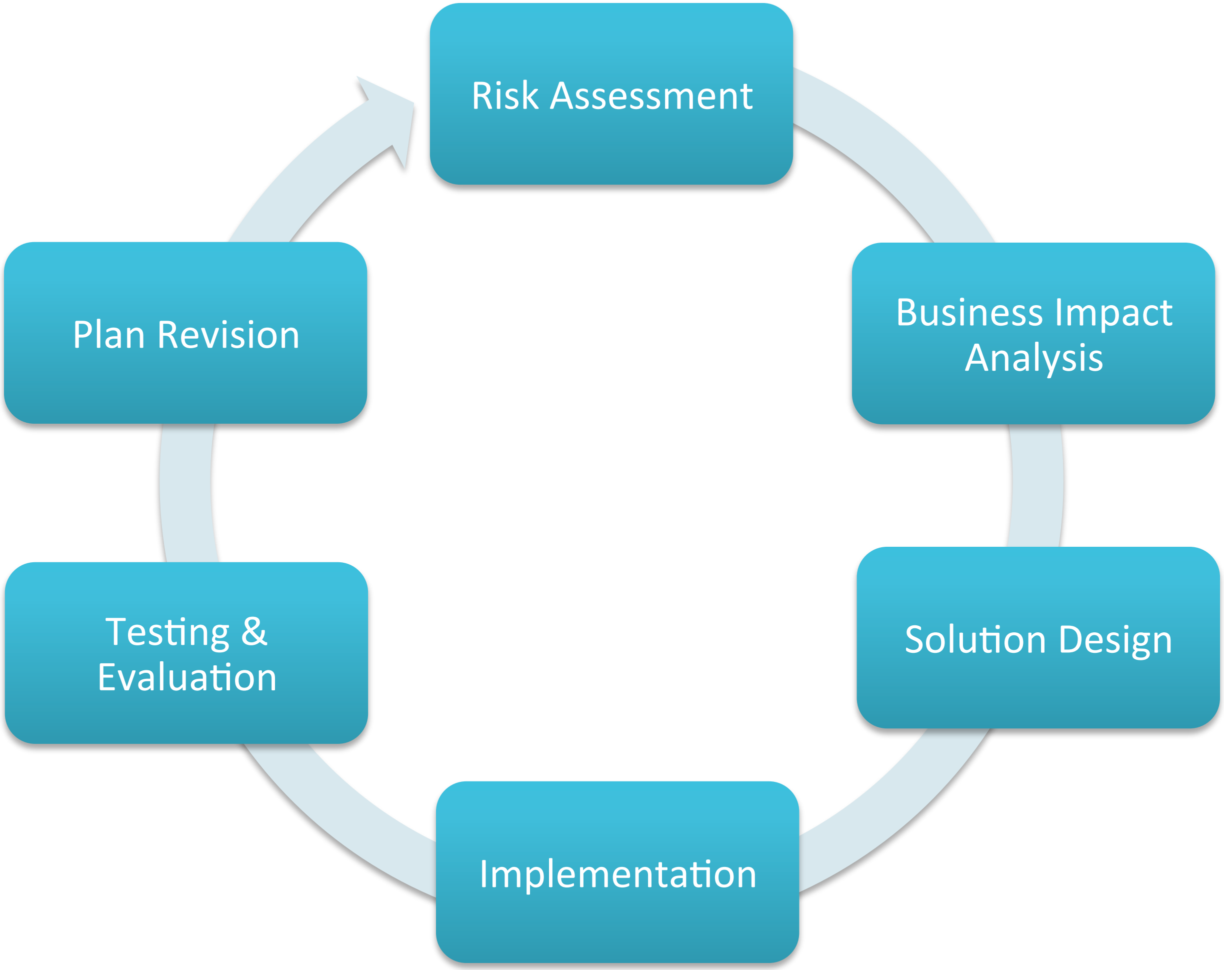
Continue critical business functions in the absence of key resources (including people: employees, customers, suppliers, regulators, and others).

Business Continuity Planning 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 that would prevent recovery
- Covering all critical company processes

Components of Effective Business Continuity Planning



Conduct a Risk Assessment

Consider the risks to your organization and the probability of each happening:

Natural

- **Earthquake**
- **Flood**
- **Hurricane**
- **Drought**
- **Twister**
- **Tsunami**
- **Cold/Heat wave**
- **Thunderstorm**
- **Mudslide**

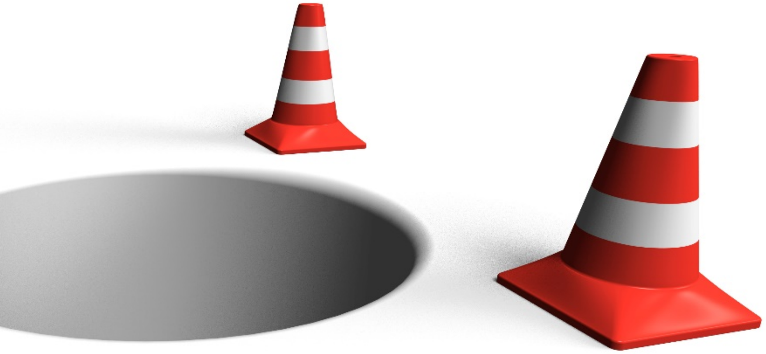
Man-Made

- **Riots**
- **War**
- **Terrorism**
- **Power outages**
- **Sprinkler system bursts**
- **Equipment sabotage**
- **Arson**
- **Epidemic**
- **Pollution**
- **Transportation accident**
- **Food poisoning**

Technological

- **Database corruption**
- **Hacking**
- **Viruses**
- **Internet worms**

Common Planning Pitfall



- You do not need to develop individual contingencies for each type of risk/disaster.
- Focus on the absence of key resources, such as (but not limited to) data, regardless of the reason.

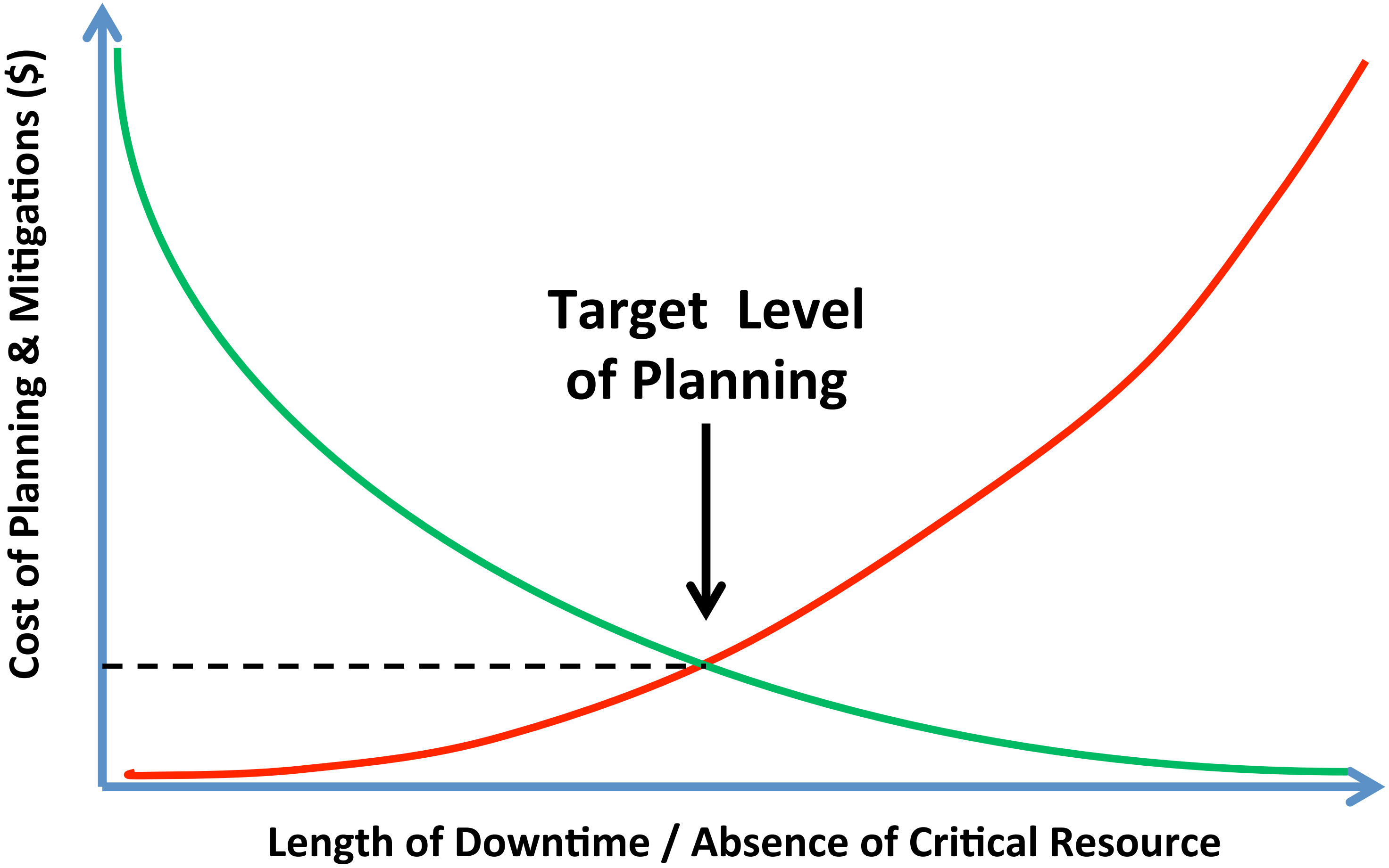
Conduct a Business Impact Analysis (BIA)

- Evaluate each key business unit to identify its:
  - Inputs
  - Process performed
  - Outputs
- Identify key resources, dependencies, and other key considerations:
  - Dependent Resources (Things *and* People/Departments)
  - Related or Dependent Processes
  - Peak Periods/Seasonality
- Request supporting data throughout

BIA - Analyze & Summarize

- Identify and prioritize business units, operations, and processes essential to the survival of the business
- For each, determine its:
  - ✓ RTO – Recovery time objectives
  - ✓ RPO – Recovery point objectives
- The results typically set the priority of planning efforts

How Much Planning and Mitigation Is Enough?

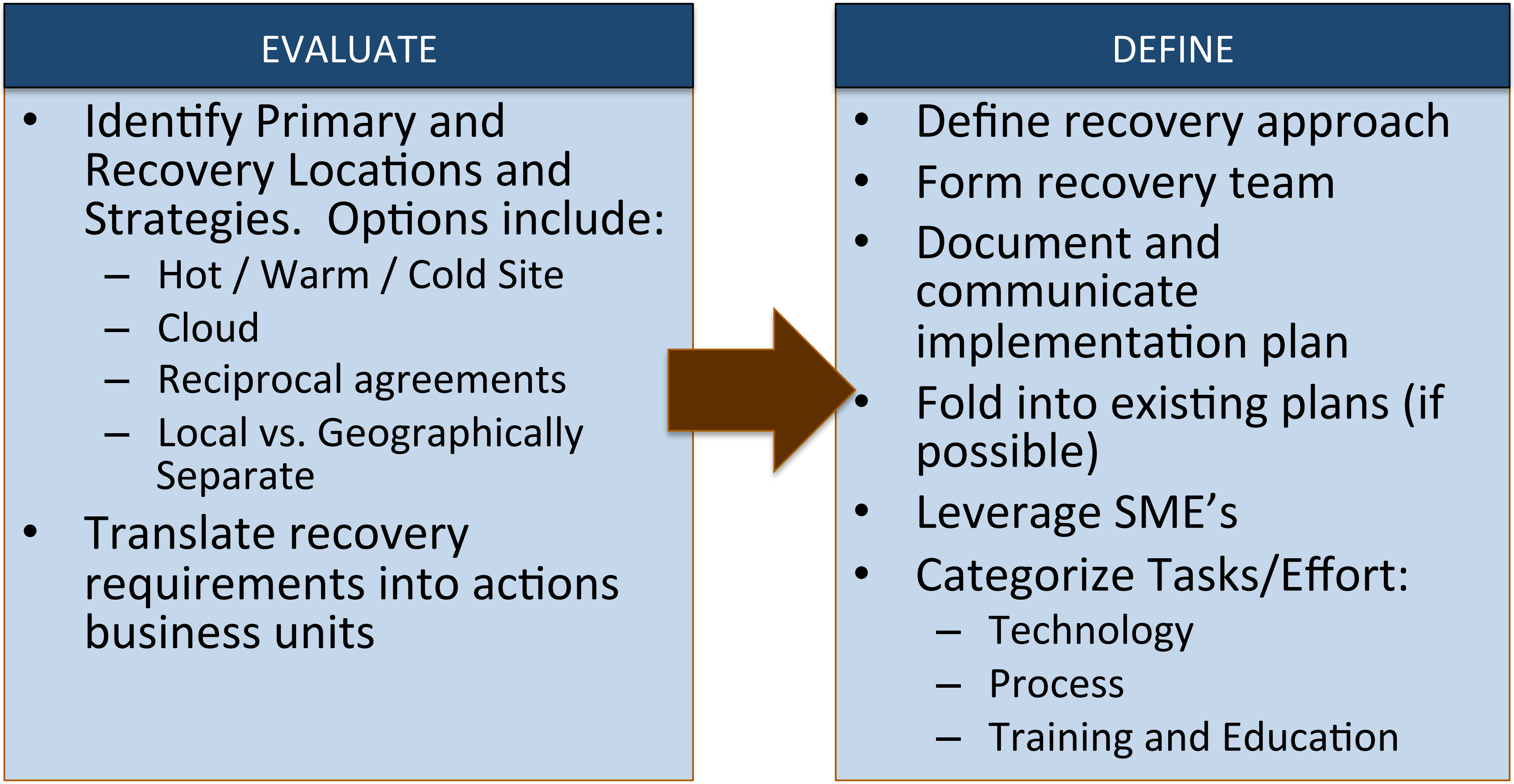


“Umbrella” Plan (Common Elements, Regardless of Business Unit)

- Roles and Responsibilities
- Disaster Management Team (Executives)
- Disaster / Continuity Operation Activities:
  - Declaration of a Disaster
  - Disaster Management (Command & Control, Status, Communications, etc.)
  - Damage Assessment
  - Equipment Salvage
  - Recovery Processes (alternate site)
  - Continuity Processes (alternate site)
  - Resumption at Primary Site
  - Declare End of Disaster
  - Post Mortem (Lessons Learned)
  - Update DRP / BCP
- Testing & Maintenance

Solution Design

Disaster Recovery Considerations



EVALUATE

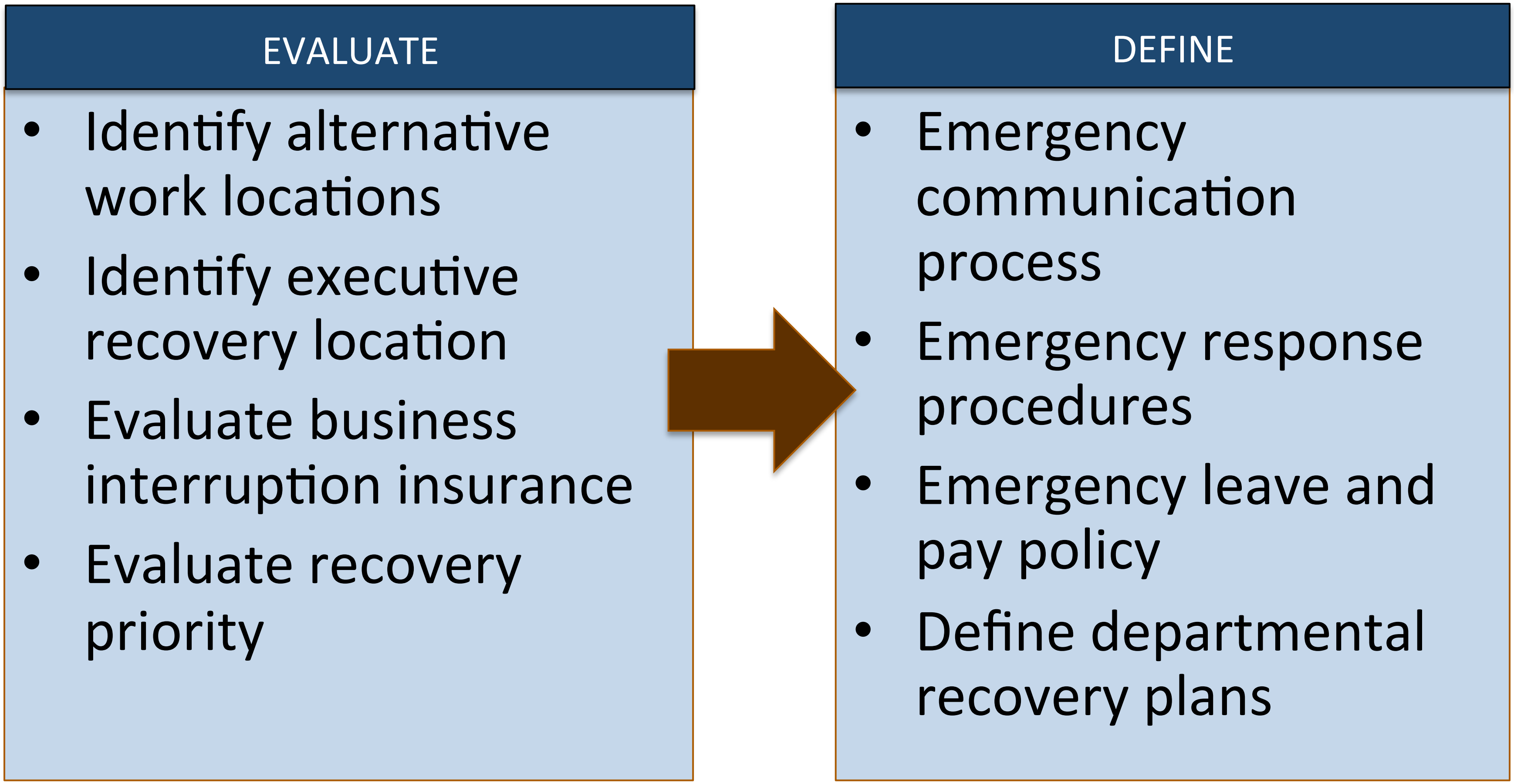
- Identify Primary and Recovery Locations and Strategies. Options include:
  - Hot / Warm / Cold Site
  - Cloud
  - Reciprocal agreements
  - Local vs. Geographically Separate
- Translate recovery requirements into actions business units

DEFINE

- Define recovery approach
- Form recovery team
- Document and communicate implementation plan
- Fold into existing plans (if possible)
- Leverage SME's
- Categorize Tasks/Effort:
  - Technology
  - Process
  - Training and Education

Solution Design

Business Continuity Considerations



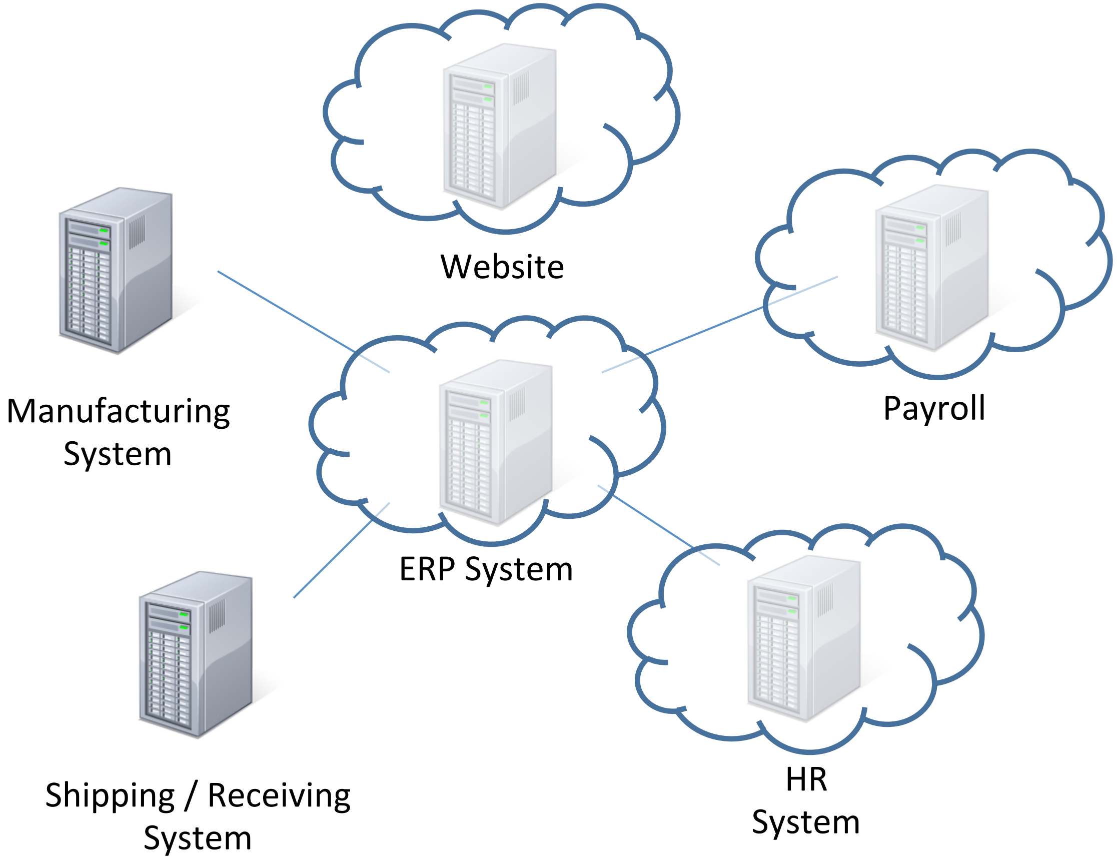
EVALUATE

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

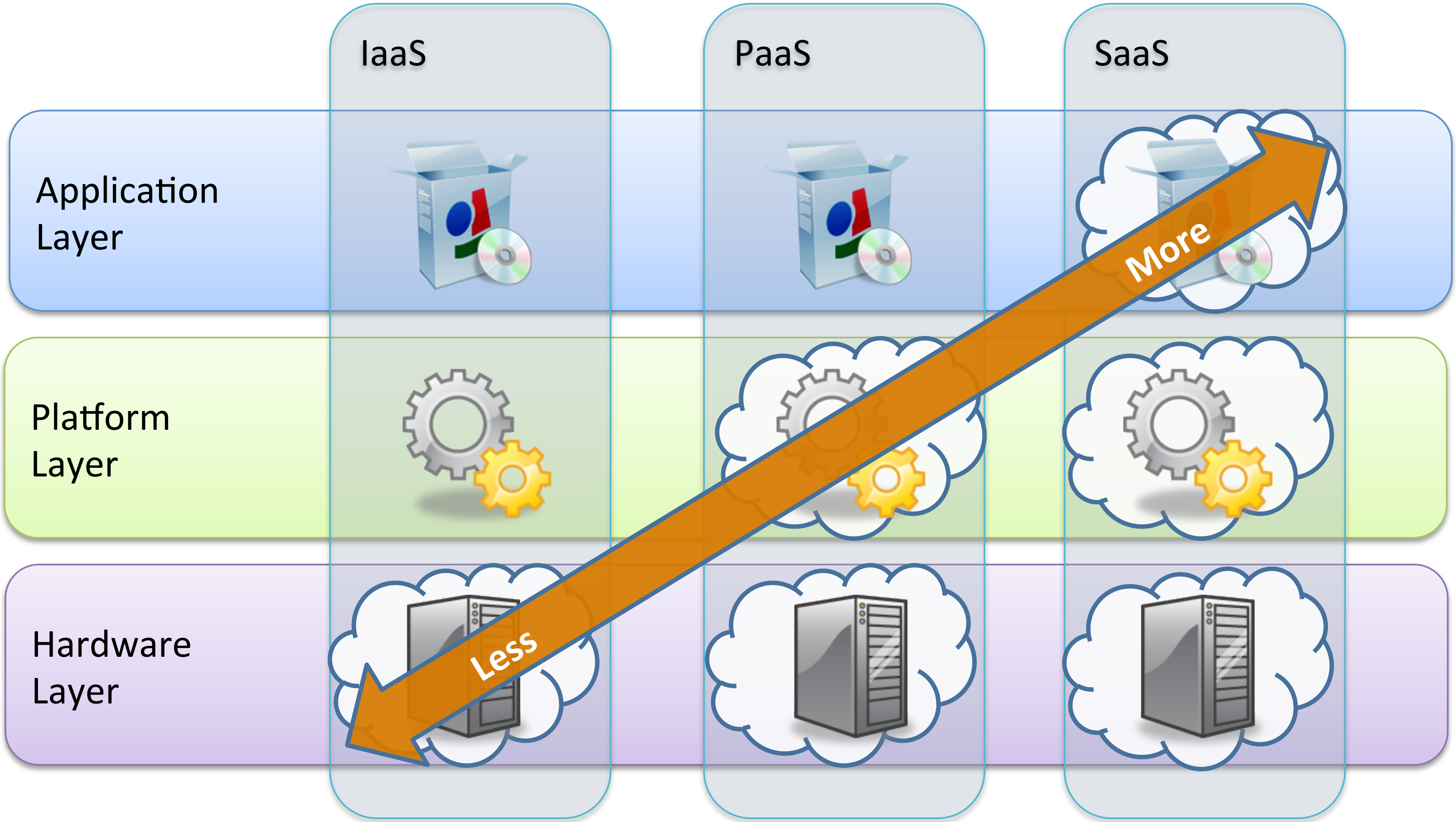
DEFINE

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

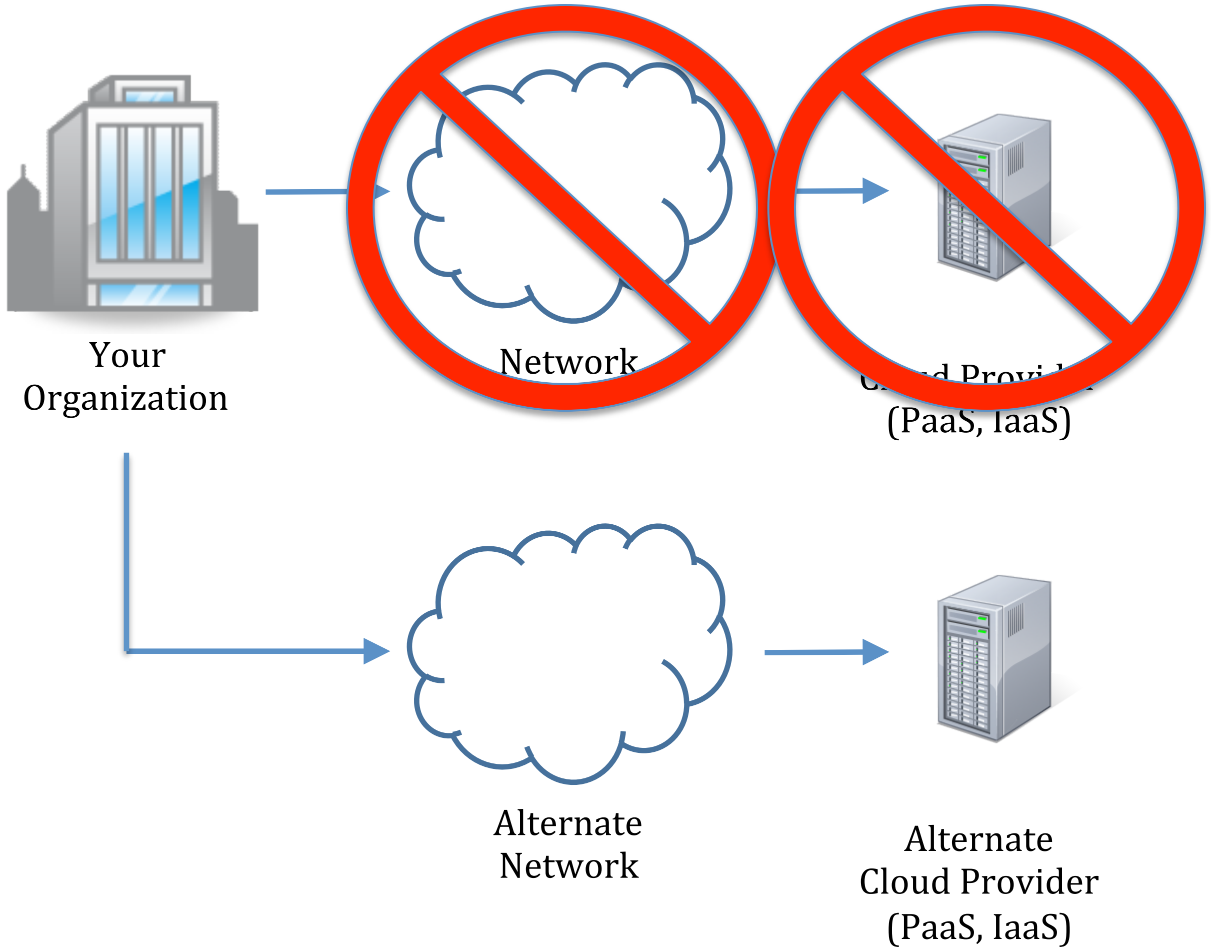
Solutions For Cloud Apps



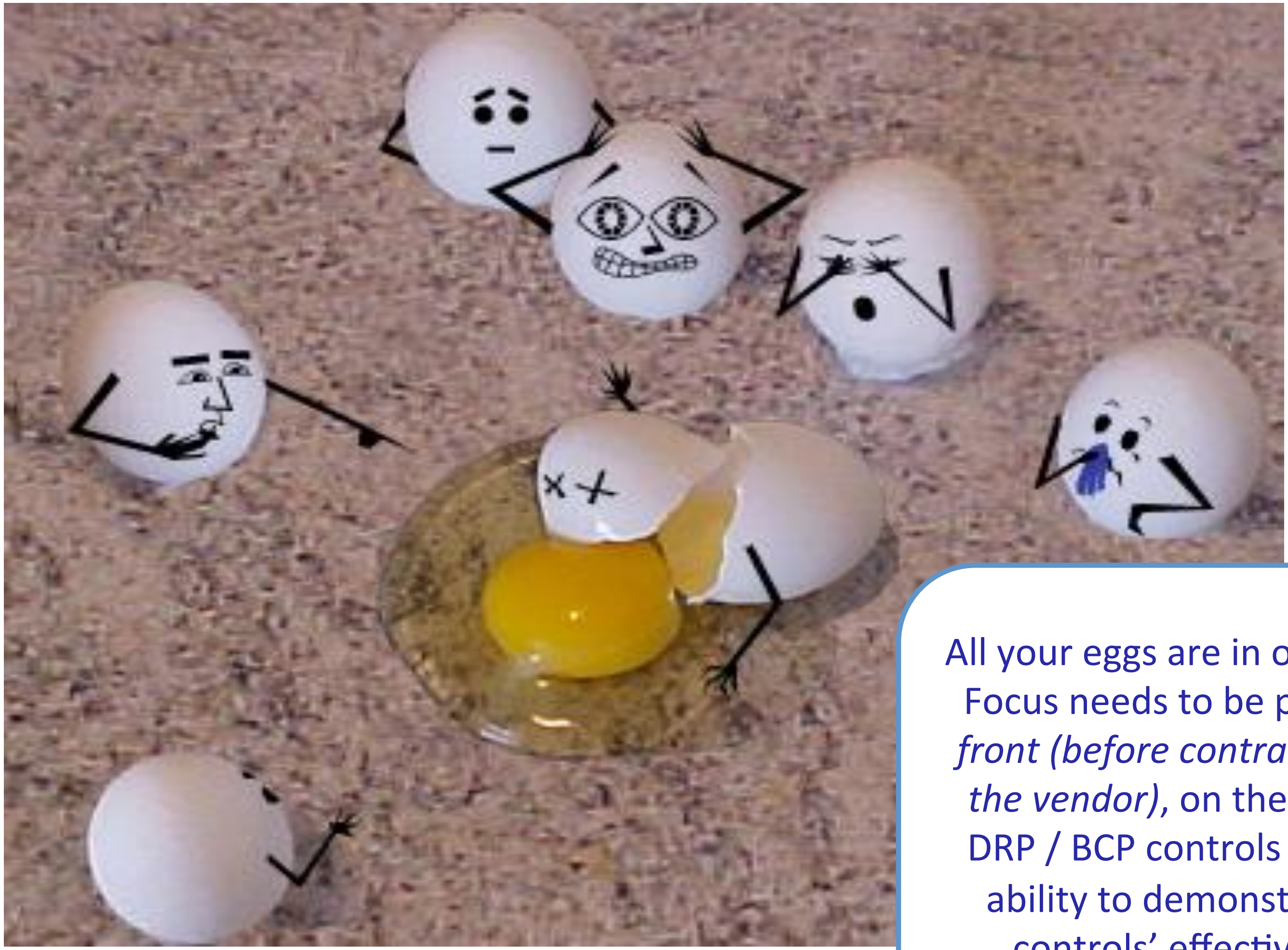
IaaS, Paas, Saas, & Reliance on Vendors



IaaS & PaaS DRP / BCP Strategy

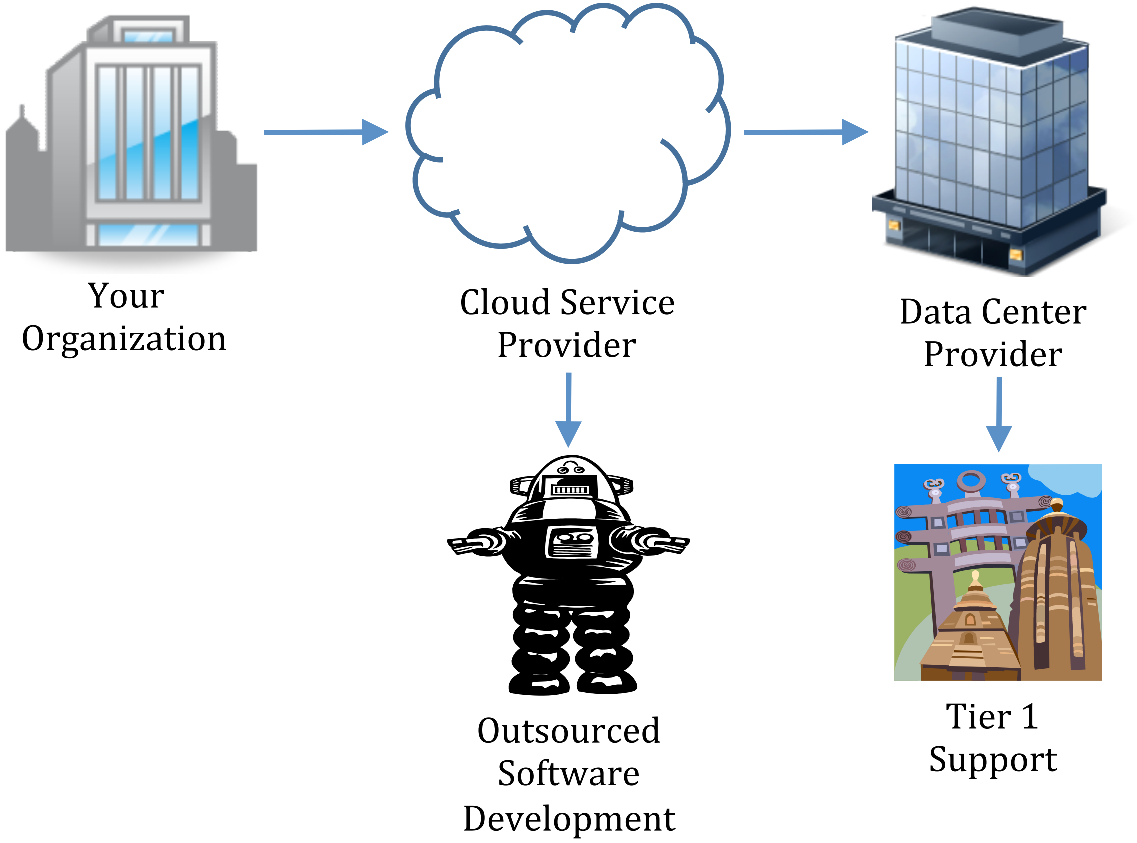


SaaS DRP / BCP Strategy



All your eggs are in one basket. Focus needs to be placed, *up front (before contracting with the vendor)*, on the vendor's DRP / BCP controls and their ability to demonstrate the controls' effectiveness.

‘Nested’ Cloud Services



Your Organization

Cloud Service Provider

Data Center Provider

Outsourced Software Development

Tier 1 Support

Cloud Consideration Summary

- If you contracted for an IaaS or PaaS service, plan for redundancy by contracting with more than one vendor
- If you contracted for a SaaS service:
  - Understand the vendor's environment
  - Understand the vendor's disaster recovery / business continuity plan
    - **BEWARE:** BCP / DRP is often separate from Service Level Agreements (e.g., guarantees of 99.999% uptime). Most SLA's also have a force majeure ('acts of God') clause. Understand what guarantees they provide regarding disaster situations.
  - Ensure ongoing compliance
    - Obtain and *review* a Service Organization Controls (SOC) report
    - Ensure there is an audit clause in your agreement
    - Include penalties if they do not meet uptime requirements

General DRP / BCP Considerations

- Key staff (and/or vendors) may or may not be available during the recovery effort
  - Plan for Primary, Secondary, Tertiary, others
  - Ensure adequate decision-making and spending authority in advance
- Communications and infrastructure for the region may/may not be functioning
- Escalation plan and related timelines

General DRP / BCP Considerations

- Recovery procedures should provide enough detailed so that alternate resources can follow if needed
- Recover all vs. subset of the required systems to meet critical (not all) business processes
- There will be performance degradation
- Functionality may be limited

TESTING AND CONTINUOUS IMPROVEMENT

Testing & Improvement

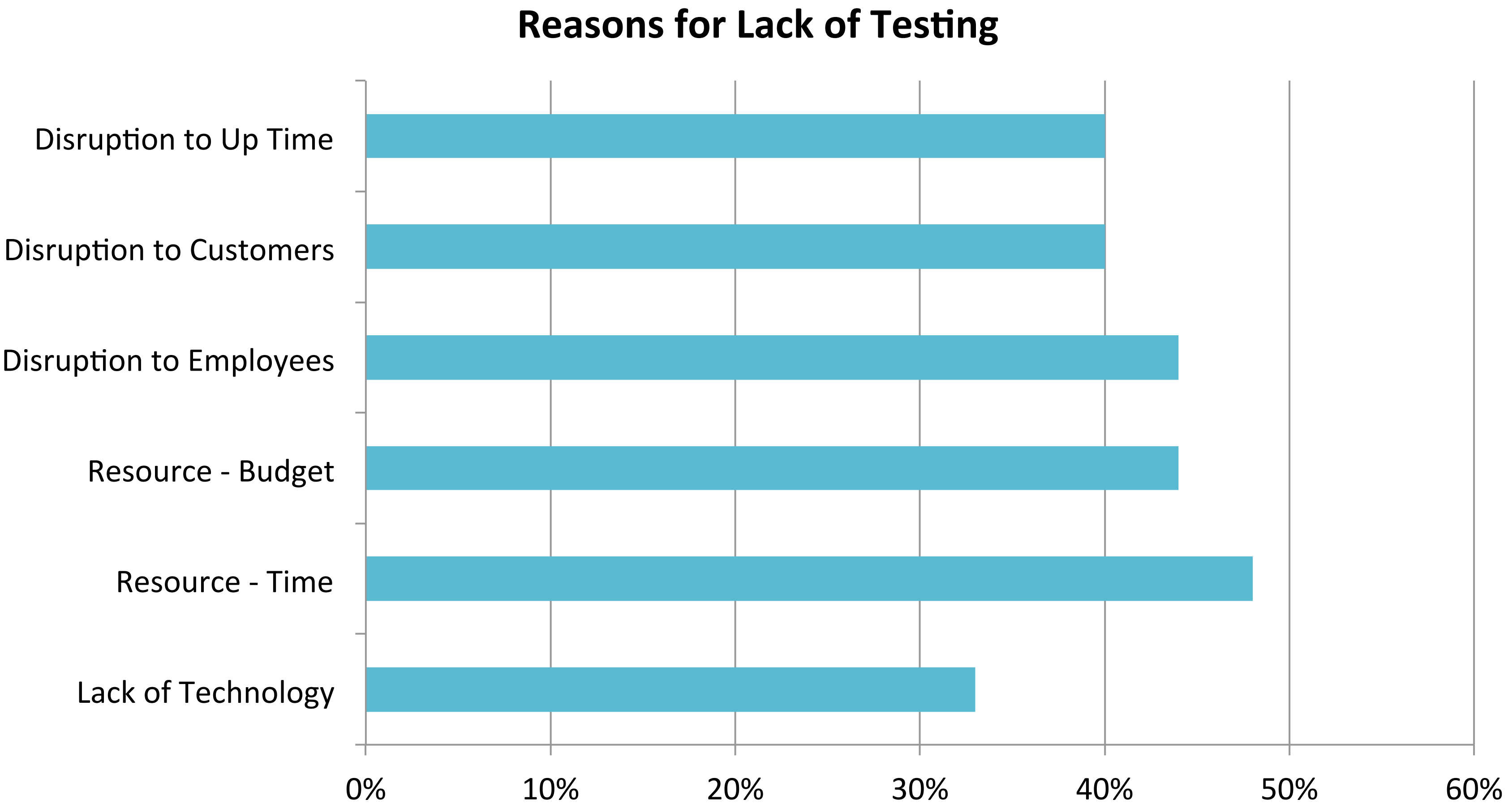
- Types of Testing:
  - Table Top Testing
  - Crisis command team call-out testing
  - Fail Over Testing
    - Technical swing test from primary to secondary work locations
    - Technical swing test from secondary to primary work locations
  - Application test
  - Business process test
  - Full Recovery Exercise
- Debrief after Testing and Update Plan(s)

Testing Decisions

- Testing type and depth is highly variable
- 18% of companies reported they perform no DRP or BCP Testing

OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...
HELP! HELP!
SOMEDAY WE HOPE TO HAVE A BUDGET.
© 2000 United Feature Syndicate, Inc.
8/15/00

Why Companies Do Not Test



Continuous Improvement

- Plan Revision
  - Evaluate Plan Assumptions and Test Results
  - Re-conduct selection of BIA Interviews
  - Update system inventory
  - Update hardware inventory
  - Determine what plan execution steps require revision
  - Revise and publish
- Ongoing Training
  - DRP / BCP Leaders
  - Company SME's
  - End User Updates (*including Audit Committee and BOD*)

TRENDS

Trends

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

AUDIT CONSIDERATIONS

Audit Considerations

- DRP / BCP Team Organization and Communication
  - Secondary, Tertiary, etc.
  - Identified and Empowered
- Risk Assessment
- Business Impact Analysis
  - RTOs, RPOs, etc.
- Cloud Vendors
  - Disaster clauses (may be separate from SLAs)
  - Service Organization Controls (SOC) Reports obtained and reviewed regularly
- Annual Maintenance

Audit Considerations (continued)

- Documentation and Distribution
  - No single point of failure (everything in one location)
  - Includes all phases identified above (declaration, damage assessment, salvage operations…declare conclusion of disaster operations, resume normal operations, perform 'post mortem' meeting, improve plan)
- Testing
  - Frequency
  - Type
  - Results
- Maturity Assessment

Resources

- NIST Contingency Planning Guide for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- Disaster Recovery Journal – drj.com
- Business Recovery Manager's Association – brma.com
- DRII the Institute for Continuity Management – drii.org

Questions?

armanino

Steve Shofner, Senior Manager

Governance, Risk, & Compliance IT Team Leader

email: Steve.Shofner@amllp.com

Office: (925) 790-2879

Mobile: (510) 681-6638