Disaster Recovery

DATA PROTECTION FOUNDATIONS

Presented by: NAME

TRAINING DAY
BY ACTUALTECH MEDIA

ActualTech Media

Agenda

- Introduction & Purpose
- Understanding DP and DR
- Components of a Strategy
- Architecting the solution
- Cloud based DP and DR
- Architecting for Cloud Recovery
- Choosing the right solution
- Next steps

Introduction & Purpose

Networking
Business
Recovery
Cloud
Disaster
Data
Backup
Storage
Analysis
File
Server
Global
Impact
Media
Service
Business Centric IT

Introduction & Purpose

DR is a process, DP is a function.

- Both critical, both require a strategy and planning to be successful
- When a disaster is declared, execution of the documented process is enacted.
  - If there is no process, there can be no consistency or repeatability. Success is unmeasurable
  - Never test your strategy in a “live” situation.

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Introduction & Purpose

DR is a process, DP is a function.

- Functions of data protection (ie. Restore/recovery), are part of the entire DR process.
    - Foundationally, a DP strategy and plan is critical to your overall recovery strategy, irrespective of where (ie. Cloud, on-prem, offsite, etc.)

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Introduction & Purpose

What makes a good strategy?

- The key components of a DR or DP strategy
- Why it is important to engage the business in the planning
- Tips to increase success during the planning process

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Introduction & Purpose

What does it mean?

- Business Impact & Recovery
- How is IT Disaster Recovery different from DR?
  - Define the differences
  - Moving forward…
- Business Centric
  - Customer Communication
  - User centered recovery

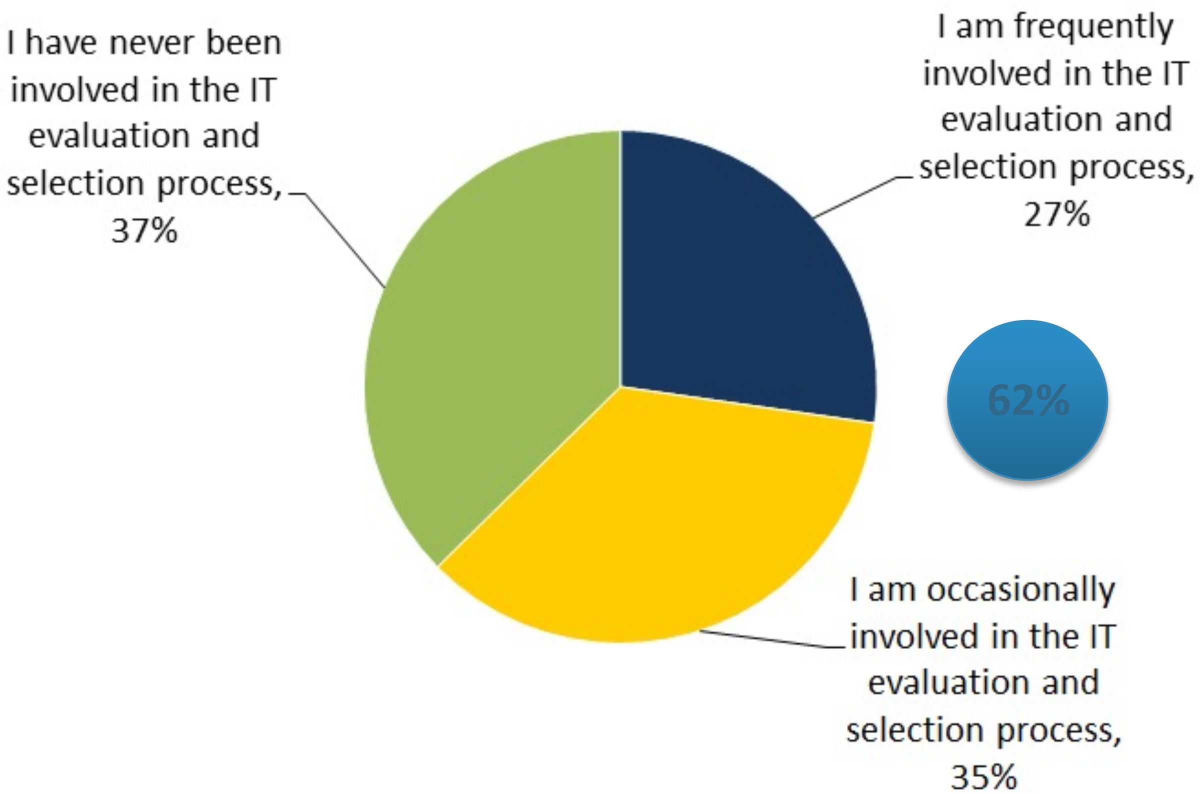
Why bother?

- My DR plan is sufficient
- We pay a PR firm to worry about it
- IT is rarely asked for input anyway

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

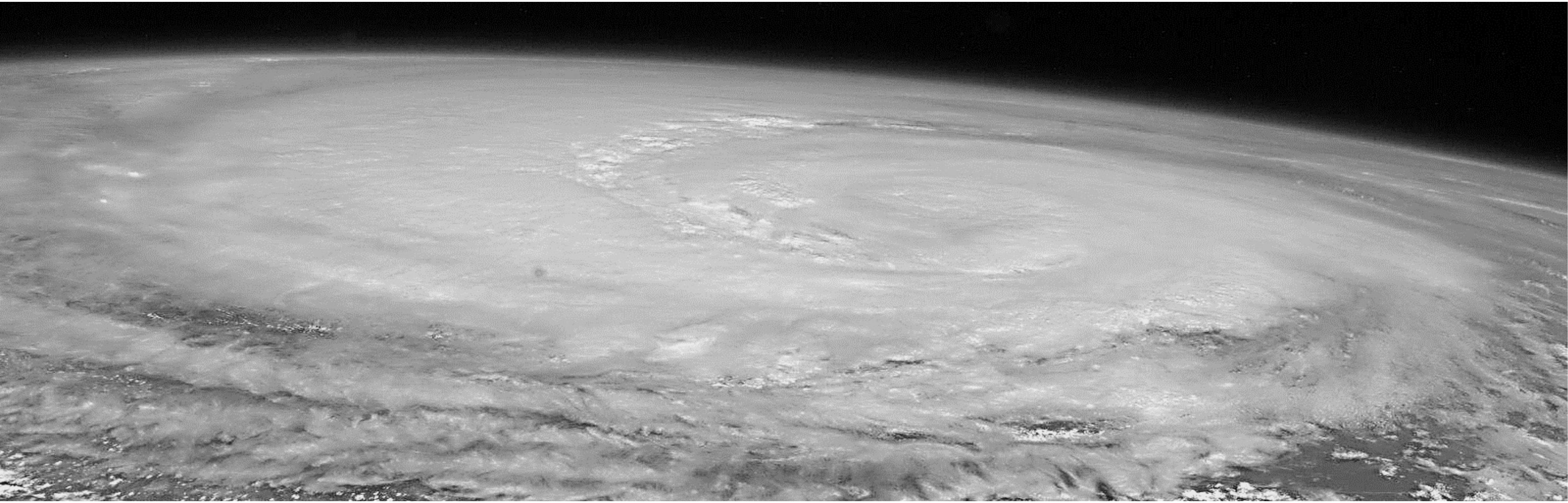
Introduction & Purpose

Please describe your role in your organization's evaluation and selection process for information technology (IT) products and services. (Percent of respondents, N=203)



Source: ESG

Understanding DP and DR



A business perspective

Understanding DP & DR

Brief History & Background

- Mainframe
    - Very centralized, “glass house”
    - Batch processes
        - Data backup
            - Reel to Reel Tape
            - Slow & Time Consuming
- Client/Server
    - Decentralized, data sprawl
        - Unmanageable
        - ”Rogue” data admins
            - Department servers outside of IT
        - Batch Process
            - Improved technology, but still time consuming

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

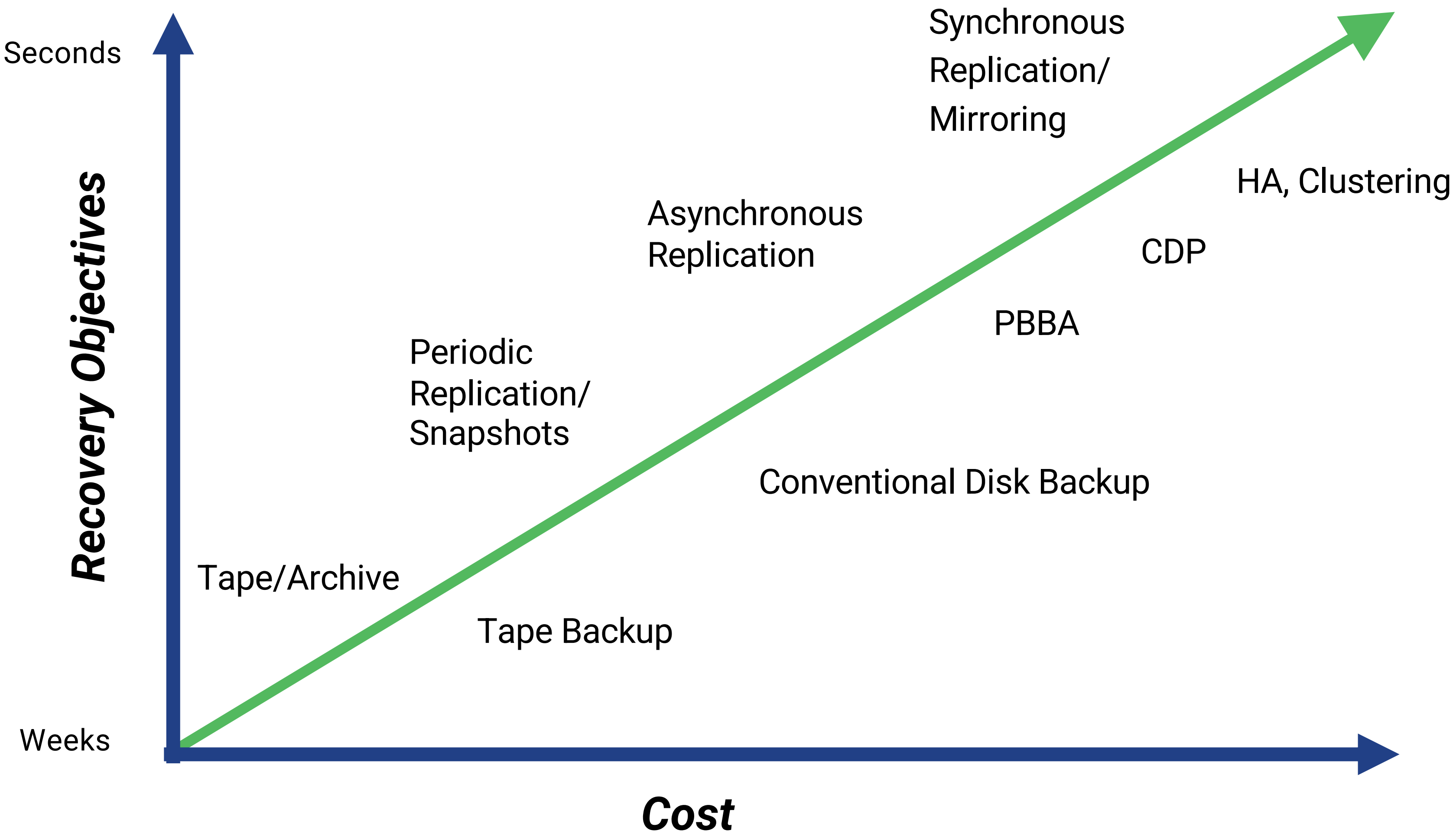
Understanding DP & DR

How it works

- Disaster Recovery
    - Recall of tapes
        - Recovery of data was slow
        - Process involved several layers of IT staff
        - Data Loss or Recovery Point inconsistent
    - Service Level Agreements <6 hours
    - Bad or malfunctioning tapes or drives wreaked havoc
- Contemporary Solutions
    - Tape finding a place with long term retention
    - Backup to disk, replication to cloud
    - Recovery to the cloud
    - Increased time to recovery, more consistent recovery points

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Data Protection Options



Understanding DP & DR

3-2-1 Rule

- Origins of the 3-2-1 rule may surprise you
  - Don’t confuse Grandfather-Father-Son
    - Rotation discipline
  - Peter Krough, digital photographer
    - 2009, after experiencing data loss he decided to have 3 copies of this data (1 primary and 2 backups), 2 on different types of media and one in a remote location, away from his normal place of business. 3-2-1
- This simple rule blurs the lines between backup and DR
  - Ensuring you follow this rule and your solution follows this rule will be a key component to your success in both restorability and recovery.

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Understanding DP & DR

Blurring the lines of DP and DR

- How do we know the difference when it seems so similar?
  - DR defines a specific predetermined amount of time you can suffer a business interruption before declaring disaster.
  - DP or simply, Backup/Restore is the function leveraged when a business interruption occurs.
    - Examples of Business interruptions
      - Corrupt file(s)
      - Deleted file(s)/volume(s)
      - Catastrophic impact/loss
    - Even in a catastrophe, if you can return to service within the pre-determined time, then you have avoided a disaster declaration

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Understanding DP & DR

Blurring the lines of DP and DR

- Approaches to Protection
    - Agentless Data Protection & Recovery (API)
    - Agent Based Solutions (traditional)
- Simply put, an API integrated solution will provide greater control and flexibility over an agent based solution.
- Agent based solutions are still required
    - Custom applications
    - Unsupported OS-type
    - Specific use case based on unique criteria

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Top Reasons For DP/DR Strategy

Example

- Parcel Service loses a customer’s digital data from one of its trucks
  - Impact: Could affect customer loyalty and trust
  - Impact: Could affect future revenue
- Cloud Backup Provider Loses Customer Backup Data
  - Impact: Subscription services may drop, customer trust diminished
  - Impact: Brand value declines, revenues drop
  - Secondary Impact: Backup Provider blames failure on disk vendor
    - Disk Manufacturer’s reputation on the line

Top Reasons For DP/DR Strategy

Example

- Financial Institution Employee Loses Tablet with PII of 10,000 cust.
  - Impact: Trustworthiness rating drops
  - Impact: Media Frenzy: Media reaches out to employee(s) for comment.
  - Lost Revenue, Lost customers, Potential litigation
- Government Contractor Inadvertently Leaks 000s of Vets SSN
  - $$/each SSN lost or leaked
  - Potential loss of future GSA contracts
- Hotel Chain’s Reservation System Goes Down
  - Impact: Future revenue lost, Customer Satisfaction drops, provides competition an opportunity to win

Top Reasons For DP/DR Strategy

April 13, 1992

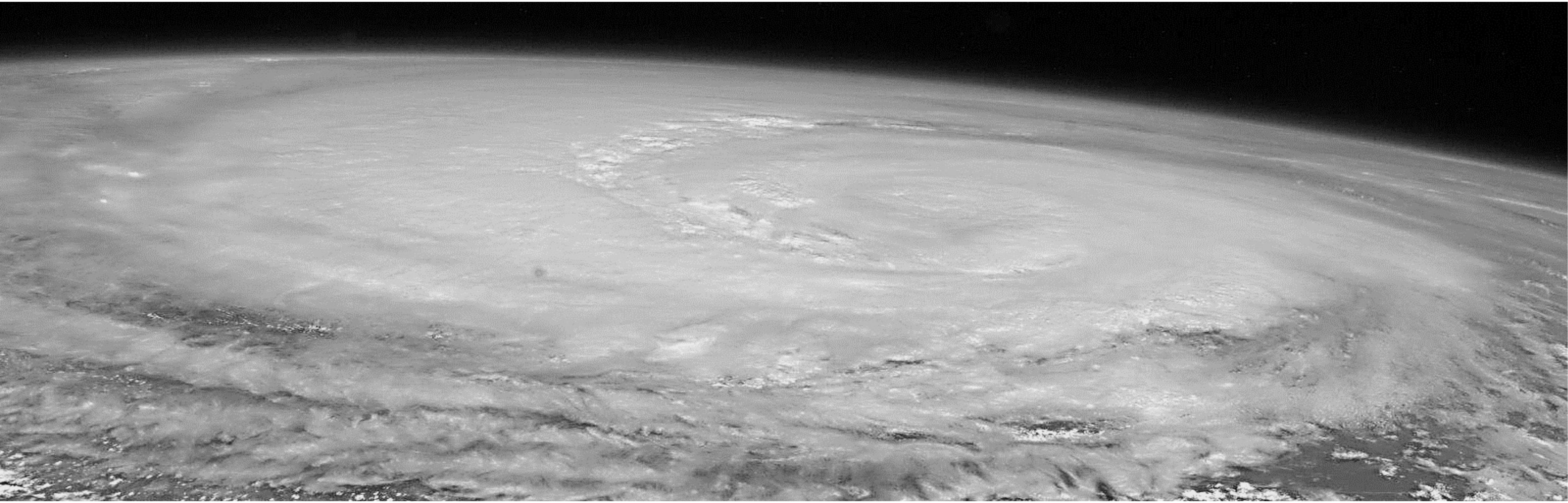
- Chicago River Underground Flood shuts down businesses for weeks
- Actual physical losses estimated at $1.95B
- Chicago Mercantile Exch shutdown lost an estimated $25B in trading
- Hundreds of small businesses never reopened.

> ***“Two out of five business experiencing a disaster, go out of business within five years. Business continuity plans and disaster recovery services ensure continuing viability”*** –Gartner

DATA protection, recovery and resumption

- Critical to IT centric recovery solution
- Business may place this secondary on its list over protecting PR fallout

Components of a Strategy



Foundational Elements

What makes a strategy?

What makes it bad?

- Failure to address the problem
  - Fixing a problem that doesn't exist
- Goals are important, but not strategy
  - Faster recovery is the goal, not the strategy
- Inability to make a decision
  - Choose a direction and move

> ***Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius—and a lot of courage to move in the opposite direction.***
> *— Ernst F. Schumacher*

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

What makes a strategy?

What makes it good?

- **Discovery**
  - You must learn or re-learn what you think you already know. Diagnosis is key to a successful strategy.
- **Scope & Boundaries**
  - Understanding the “box” within this project exists is important. Creep happens. Stay focused on the dynamics you are capable of changing.
- **Defined Steps**
  - What specific actions will you take to achieve change within the system or process you are addressing. Is it feasible? Will it be sufficient?

Fools ignore complexity. Pragmatists suffer it. Some can avoid it. Geniuses remove it.
— Alan Perlis

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Data Protection & Disaster Recovery

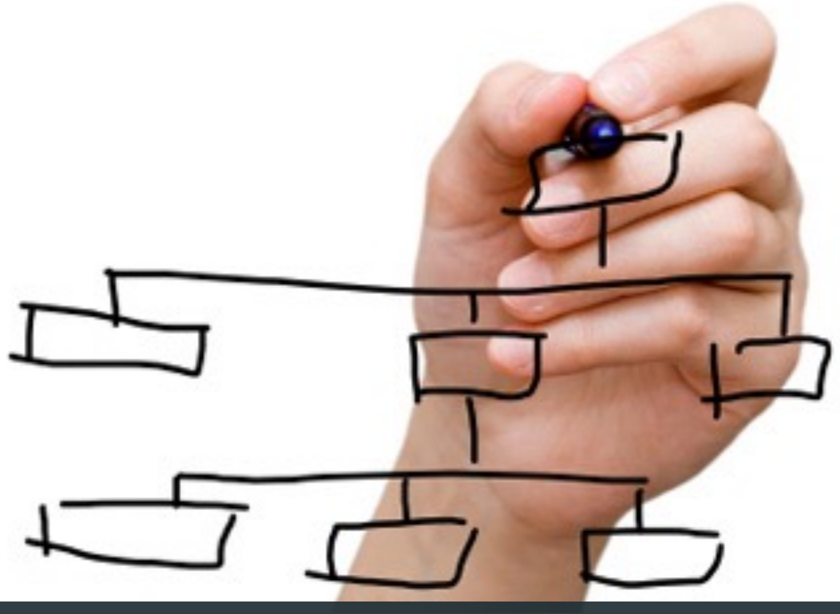
Align top line goals with Corporate Goals

Understand the business and its specific needs

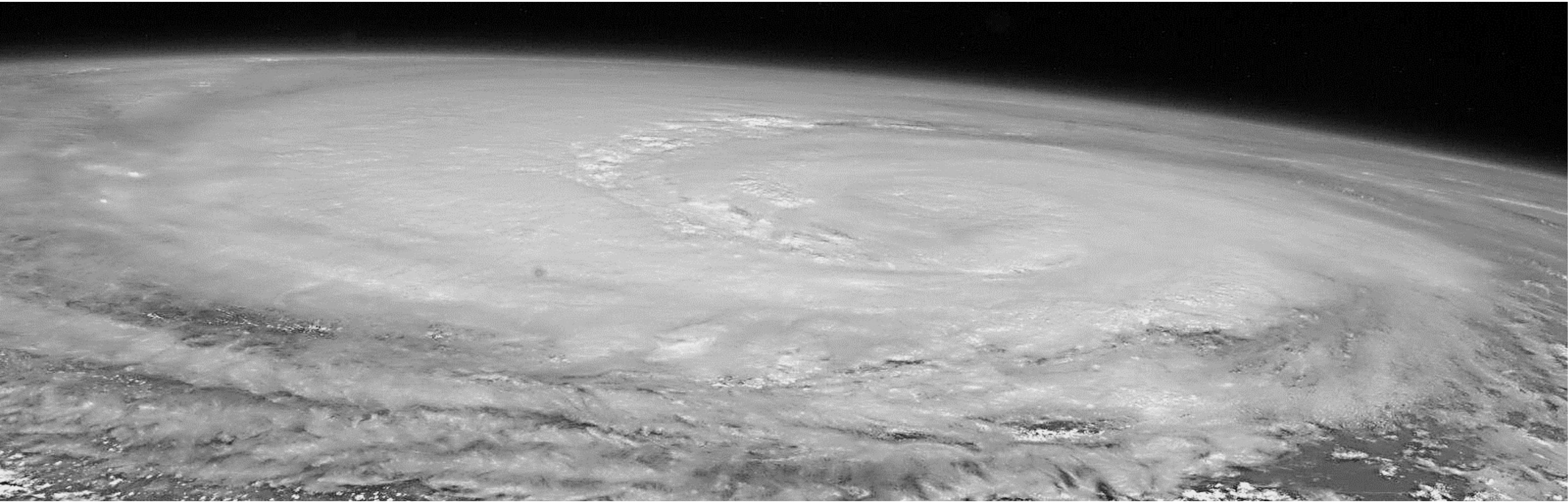
- SmB: The business and corporation potentially are the same
- Mid-Large: Multiple business units make up the entire corporation
- Clear picture of FY initiatives & how IT will support

IT Centric Recovery v. Business Centric Recovery

- May be very different objectives
- IT: System and Data focus
- Business: Customer and Public Relations Focus



Architecting a Solution



Foundational Elements

Architecting a Solution

Start with the basics

- Staff
- Business Objectives
- Key Requirements
- Recovery Needs
- Solution Assessment
- Communications Plan
- Building the strategy

Planning and preparation are the keys to a successful data protection strategy

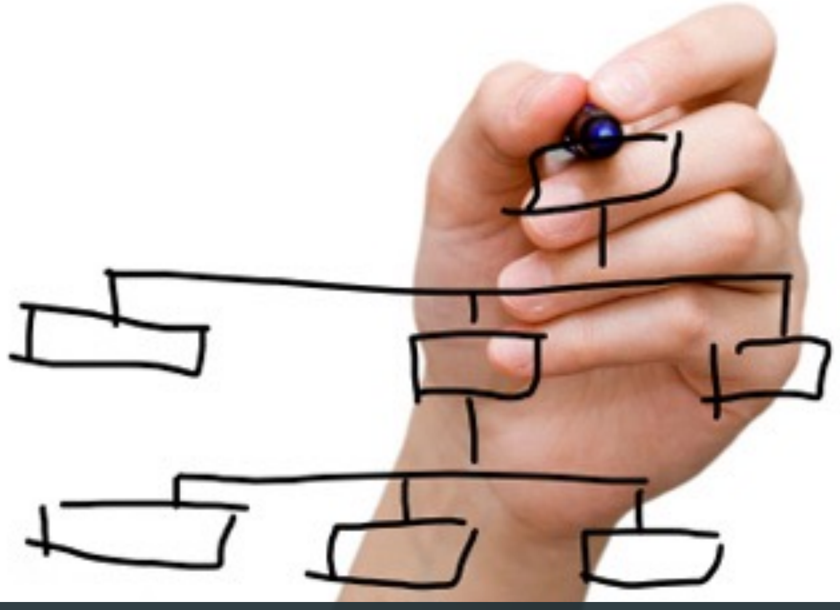
IT Self Assessment

Can you meet the business recovery expectations?

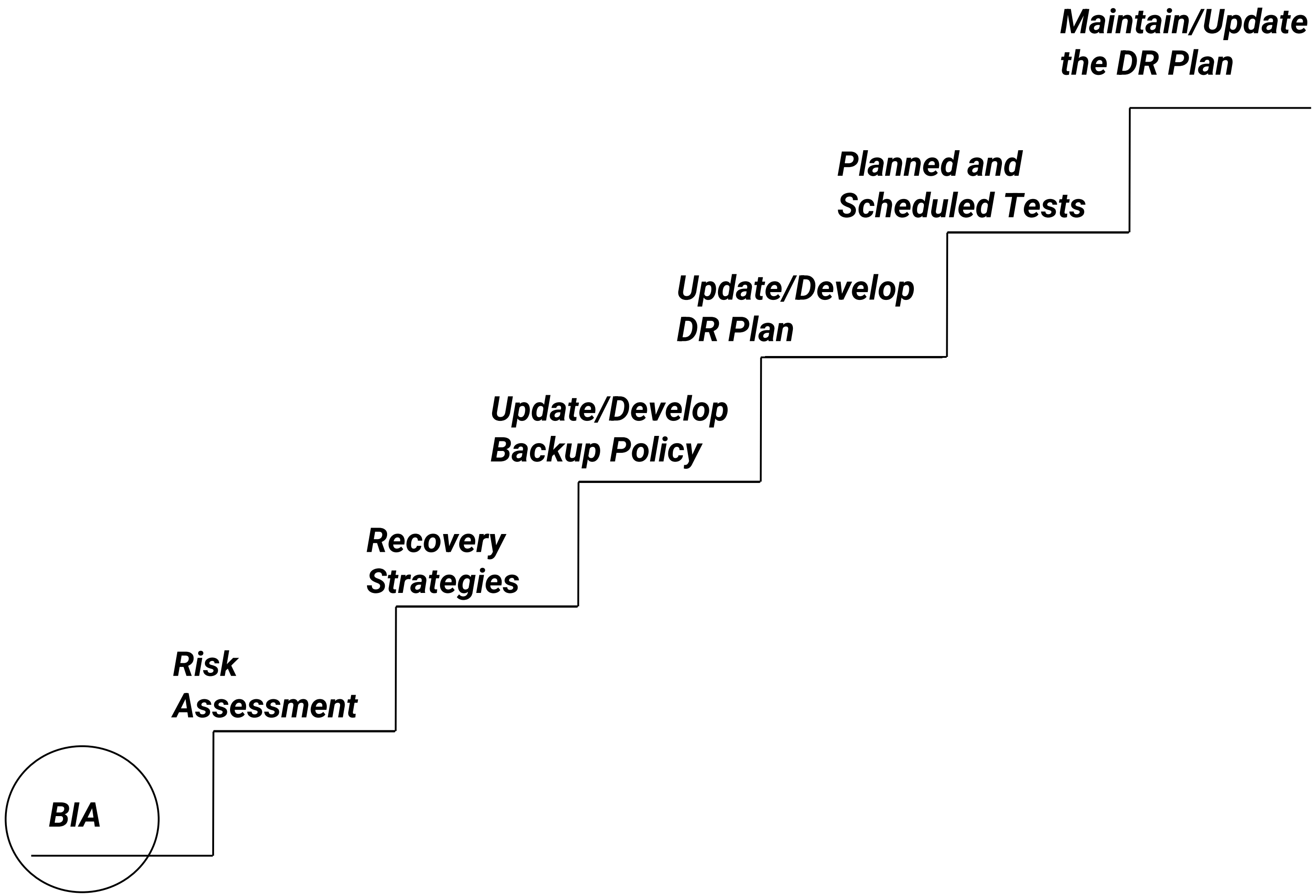
Do you have the resources, staff and support?

What recovery workloads are candidates for cloud?

What gaps could be filled with additional headcount?



Business Objectives



BIA

Risk Assessment

Recovery Strategies

Update/Develop Backup Policy

Update/Develop DR Plan

Planned and Scheduled Tests

Maintain/Update the DR Plan

**"Implementing Backup and Recovery", Wiley and Sons*
David B. Little and David A. Chapa

Business Objectives

- Customer Satisfaction
- Beating the Competition
- Generating Revenue and Profit
- Growth

IT Objectives

- Customer Satisfaction
- Deliver competitive service
- Support systems and applications
- Thrive to expand capabilities

Different functions, very similar goals

IT

Customer Satisfaction

Deliver competitive service

Support systems and apps

Thrive to expand capabilities

Business

Customer Satisfaction

Beating the Competition

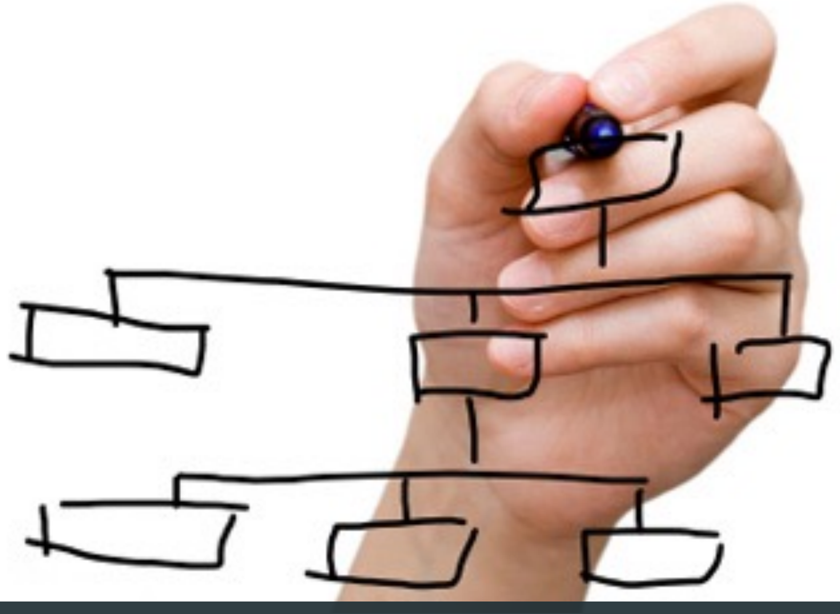
Generating Revenue and Profit

Growth

Business Objectives

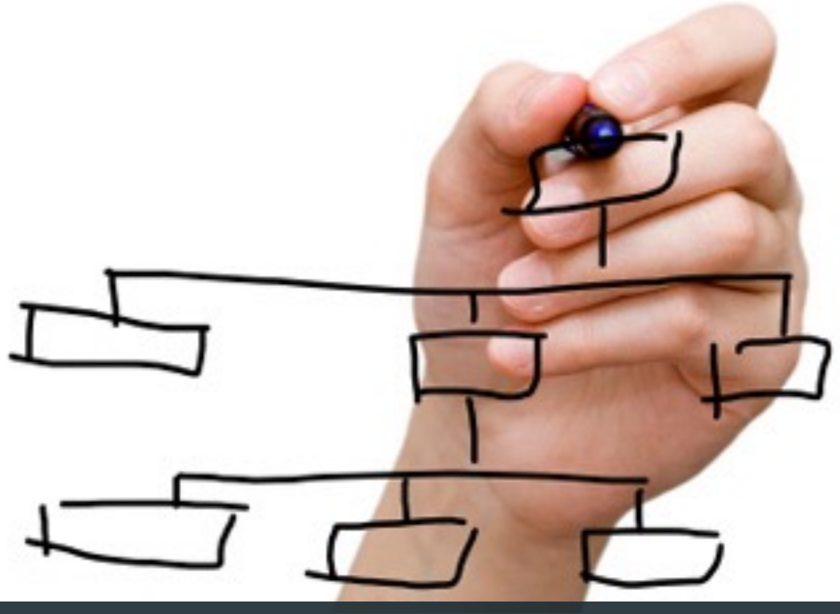
Think like a CEO

Risk Assessment, Recovery Strategy, Customer Relations, HR/Employee Relations, Investor Relations, Public Relations, Supply Chain, Communications Plan



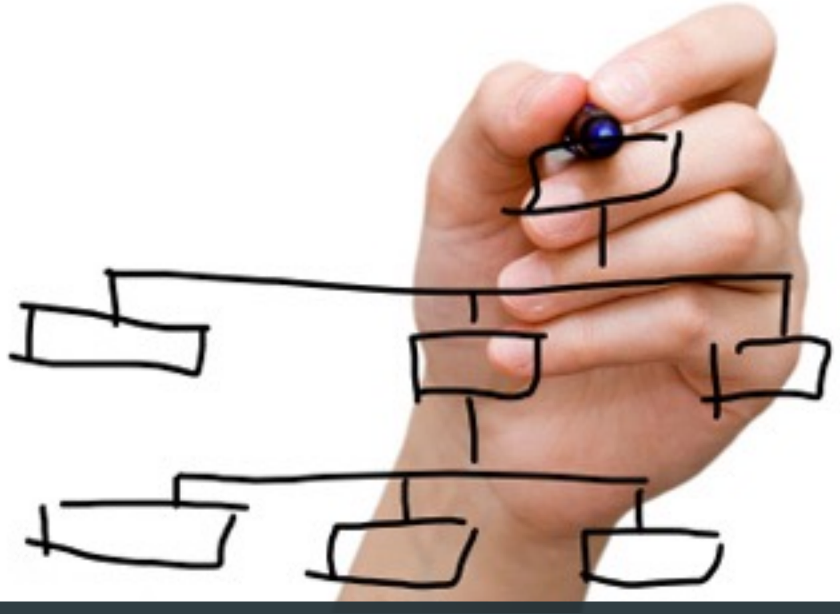
What’s the mission of the business?

- Identify the Business Units (BU) in your company
  - Understand the BU’s top line goals and initiatives
  - Prioritize Business Units, Systems
  - Uncover the primary function
    - Applications
    - Systems
    - Platforms



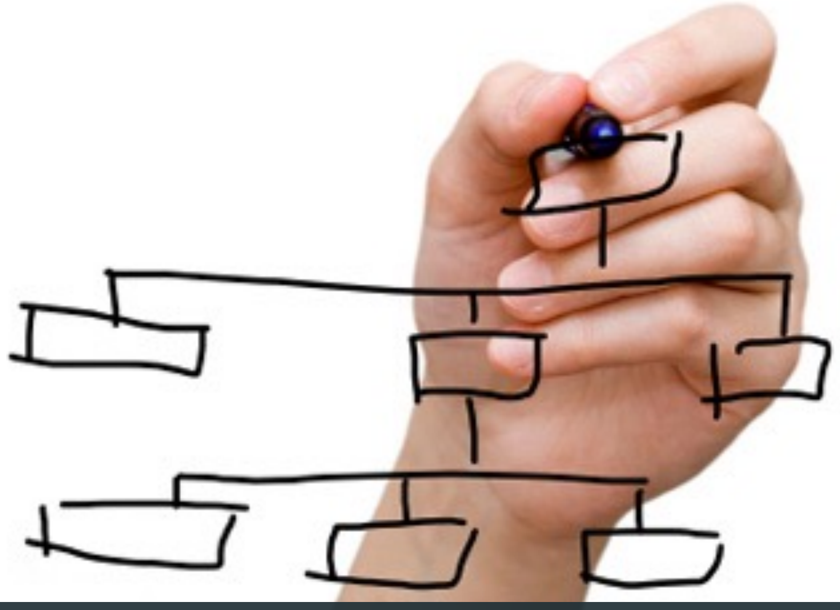
What’s the mission of the business?

- What do we do, that if we didn’t we’d be out of business?
  - Don’t be afraid to ask the obvious question
  - Create disaster simulations to better understand the recovery needs
  - What applications do you need for that mission to be successful?



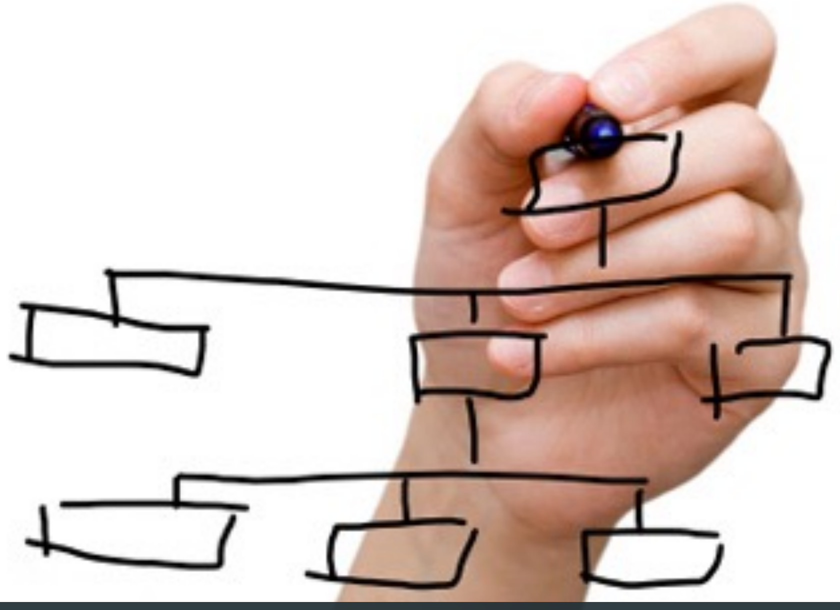
What’s the mission of the business?

- What do we do, that if we didn’t we’d be out of business?
    - Where does the data exist to support this mission?
    - Who are the “power users” of these applications?
    - Who is the primary data owner?
    - Work with the BU to determine priorities for recovery



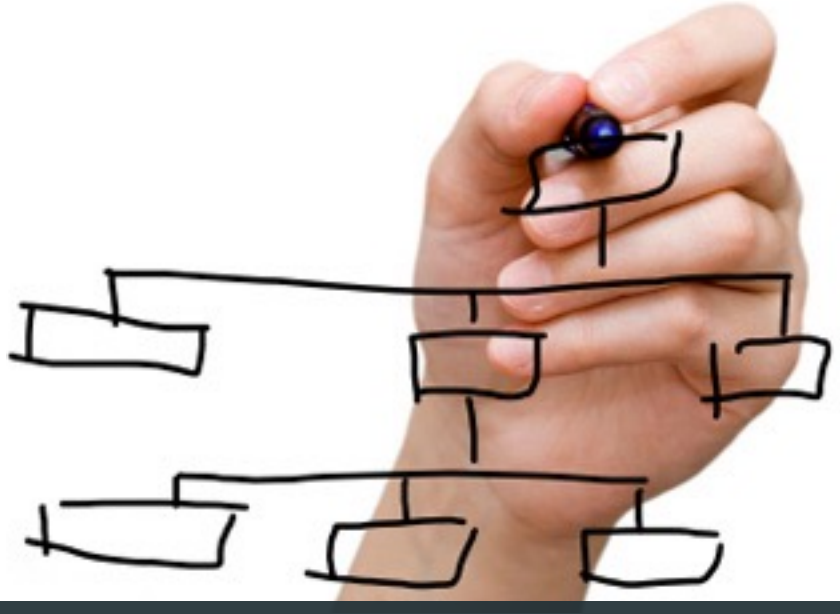
What’s the mission of the business?

- “Think like a journalist” – Interview the BU
    - Don’t assume you know what is important
    - Act like a vendor providing a service
    - Literally, no such thing as a dumb question



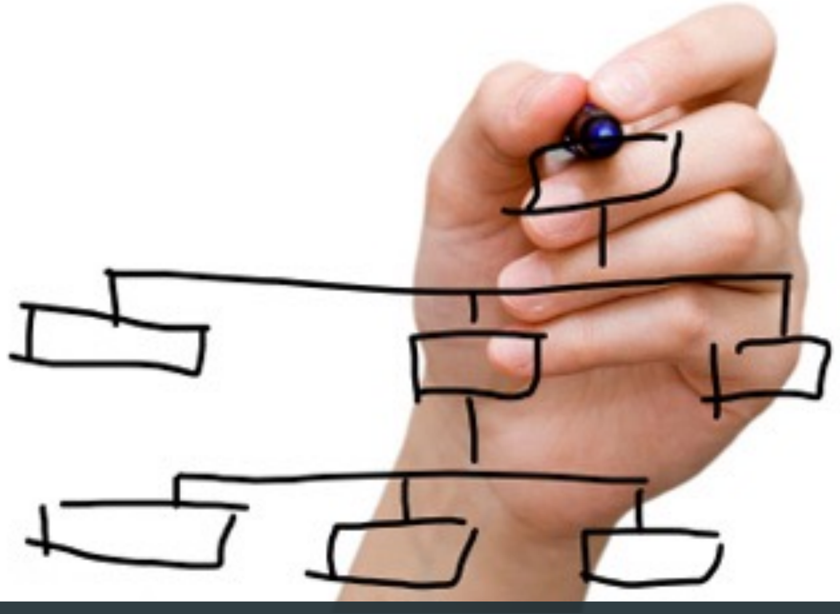
What’s the mission of the business?

- IT perspective: Identify key stakeholders
  - Data owners
  - Storage Admins
  - Backup Admins
  - Network and Security Admins
  - Business Unit Mgrs/GMs
    - Who has sign-off
    - Final approval
    - Sponsorship
  - Vendors/Partners



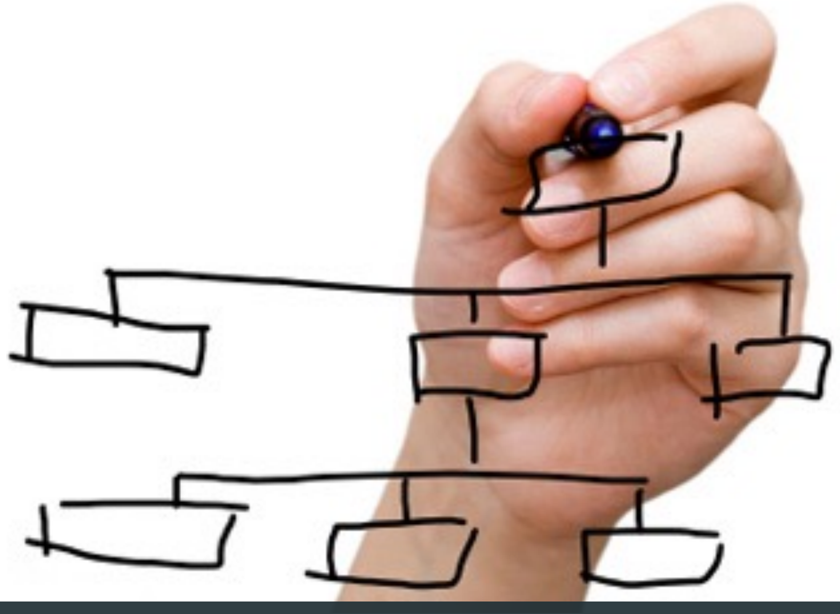
Architecting the Solution

- What needs protecting
- What is protected
- Where are you gapped?
  - Identify Protection Gaps
  - Unprotected critical data on Laptops
    - Unsecured Desktops



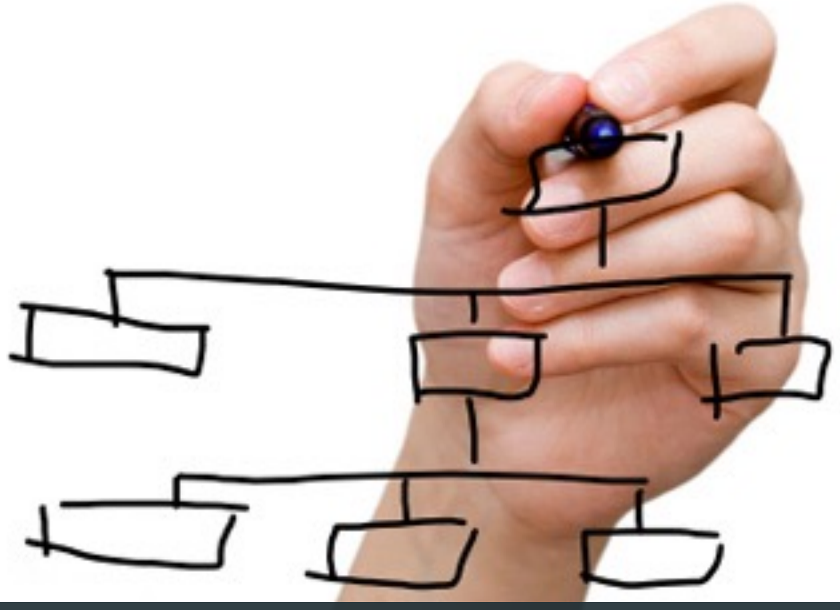
Architecting the Solution

- Remote Access Requirements
- Order of Recovery
- Cloud, On Premise, Hot Site?
- DR Team and Tasks
  - Very important to have primary and secondary roles
  - Critical to review this plan when IT turnover occurs



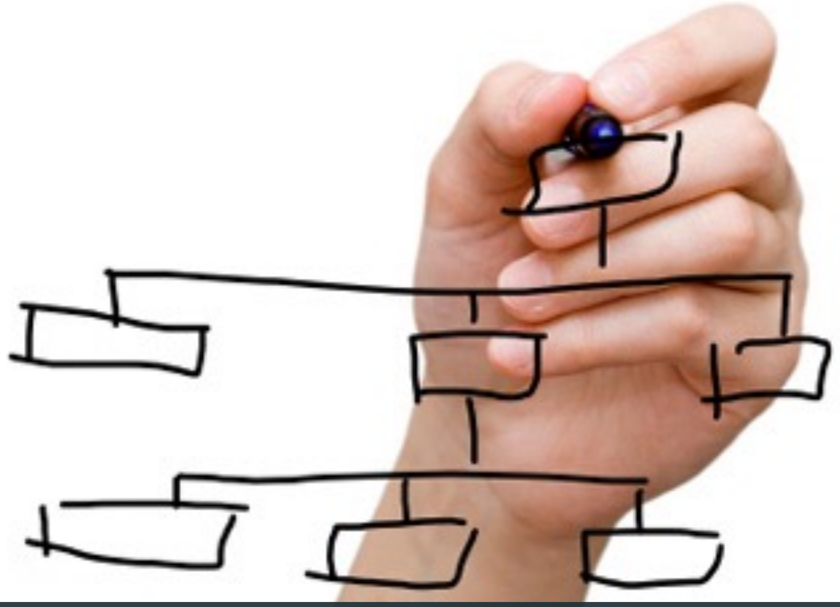
Architecting the Solution

- Identify recovery heat index
    - Using the Business Impact Analysis
        - Cost vs. Loss of unprotected Data
        - Cost vs. Access to unsecured Data
        - Applications and Systems
- Classification Framework
    - Application/System/Data
        - Mission Critical
        - Critical
        - Deferred



Architecting the Solution

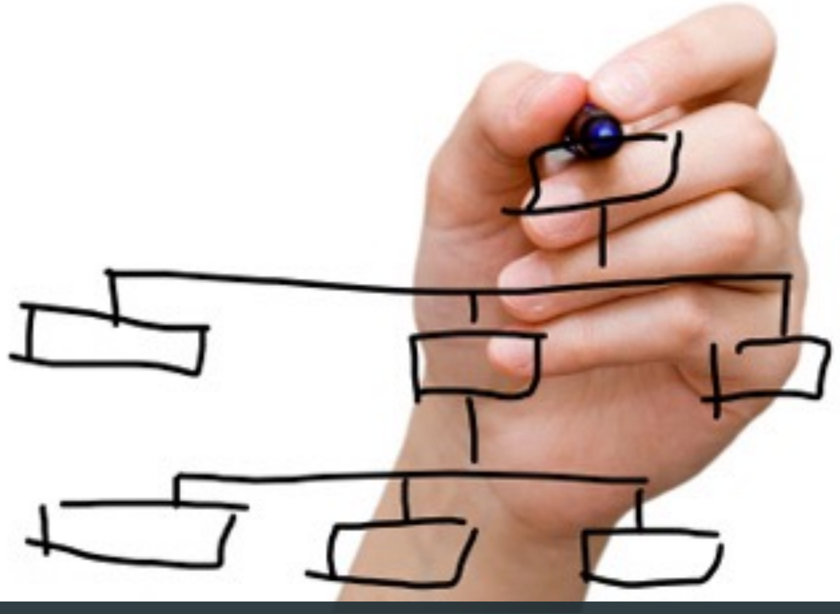
- Audit Process
  - Subscribe to 3rd Party Validation Service
  - Use a DR service provider
  - Avoid self-audits
- Regularly scheduled tests and trials
  - Measure results
  - Action plan to improve or enhance



Architecting the Solution

- Recovery KPIs – use the SMART approach
    - **S**pecific
    - **M**easurable
    - **A**chievable
    - **R**ealistic
    - **T**imely

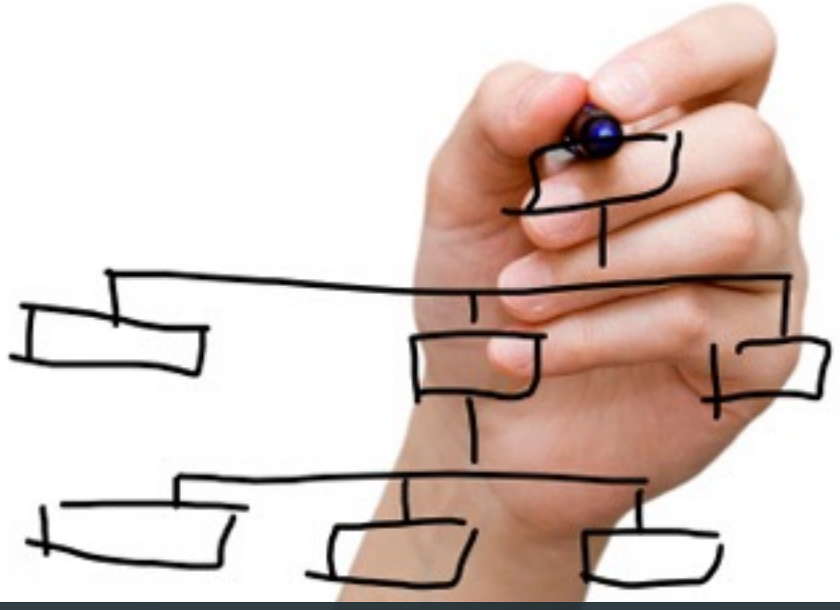
What's measured improves
– Peter Drucker



Architecting the Solution

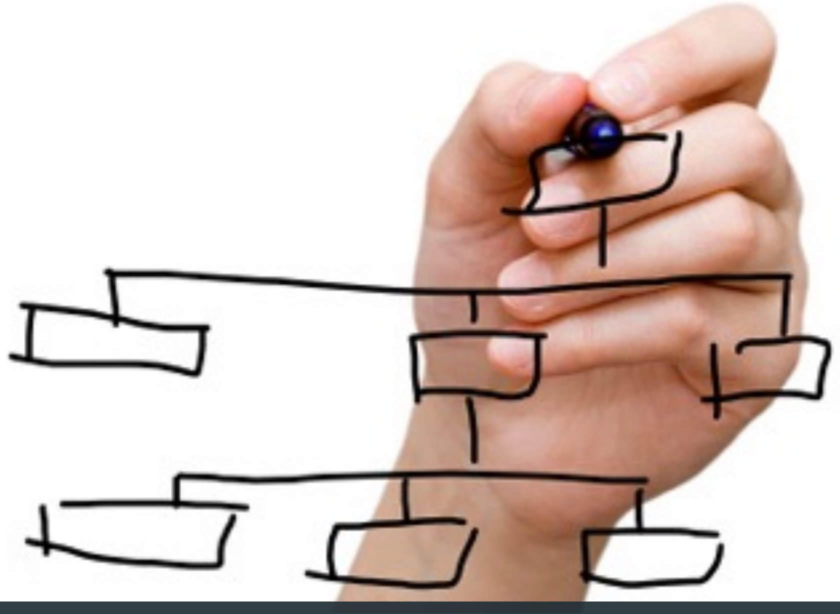
- Examples
  - Time from declaration to DR execution
  - DR Test/Result/Audit
  - Time to “business as usual”
  - Time to Tier 1 system resumption
  - Customer Satisfaction Rating
    - Within 3 months of DR
  - Revenue Impact Analysis

What’s measured improves
– Peter Drucker



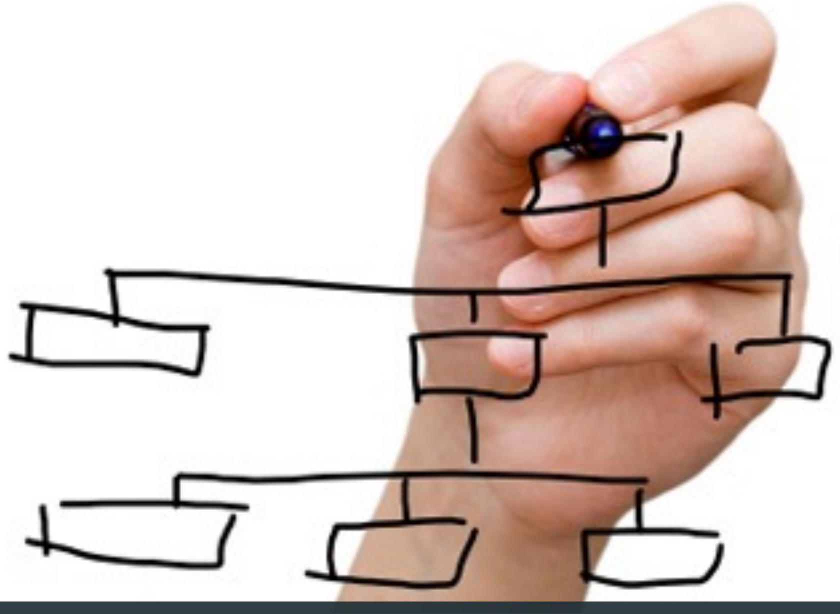
Architecting: Communication Plan

- Communication Plan
  - Work closely with your PR firm
  - Communication is key to maintain control of media
  - Who to include?
    - Employees, Customers, Vendors
    - BOD, Shareholders, Investors



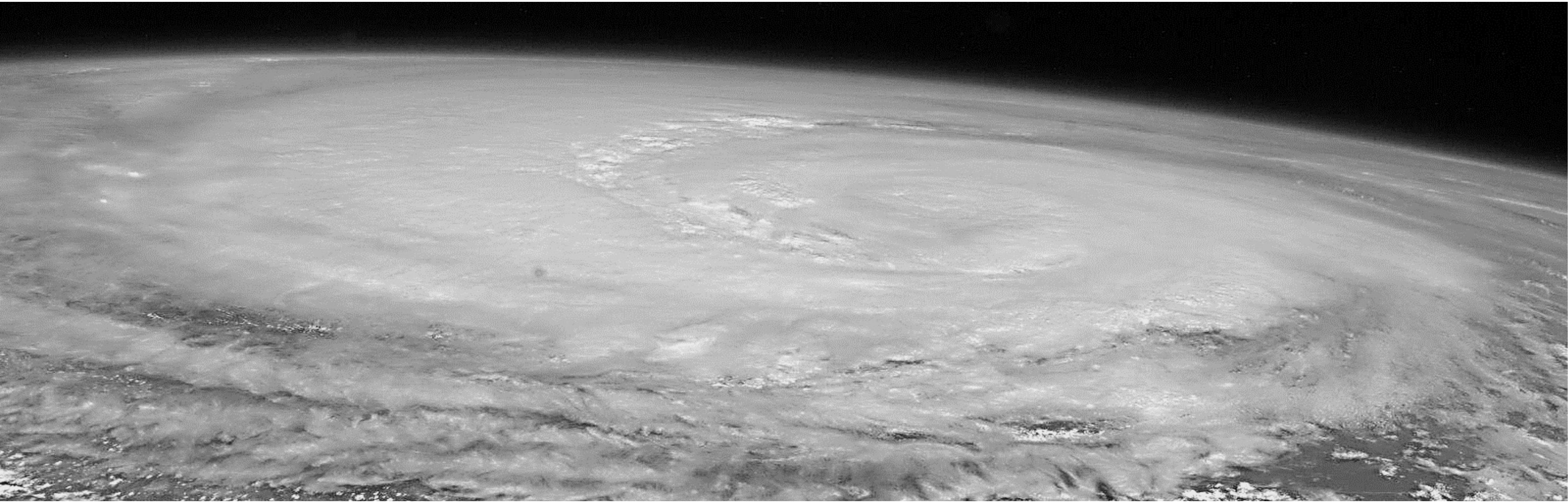
Components of a Strategy

- Media Training
  - If you are contacted by the news or press
  - Know what you should say, should not say
  - When in doubt, say nothing



When you initiate the communication, you remain in control.

Cloud Based DP & DR



Next Generation Protection

Cloud for DP and DR

Principles of the Strategy

- All of the principles of building a strategy apply whether in the cloud or on prem
- Cloud presents more of a challenge due to network constraints and volume of data
- Recovery Time Objectives may vary with cloud solutions simply based on network.
- Recovery within the cloud to compute in the cloud may be an option to expedite uptime for endusers.

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

Cloud for DP and DR

Achieving success

- All in or hybrid?
  - Data and compute all exist in the cloud
  - Data and compute on prem with recovery in cloud
  - Data in the cloud, compute on prem
- It is all about the network
  - Know your bandwidth, your guarantees, and SLAs
  - How much data must be moved to the cloud, daily?
  - Choose your solution based on its ability to consistently trickle data to the cloud incrementally

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

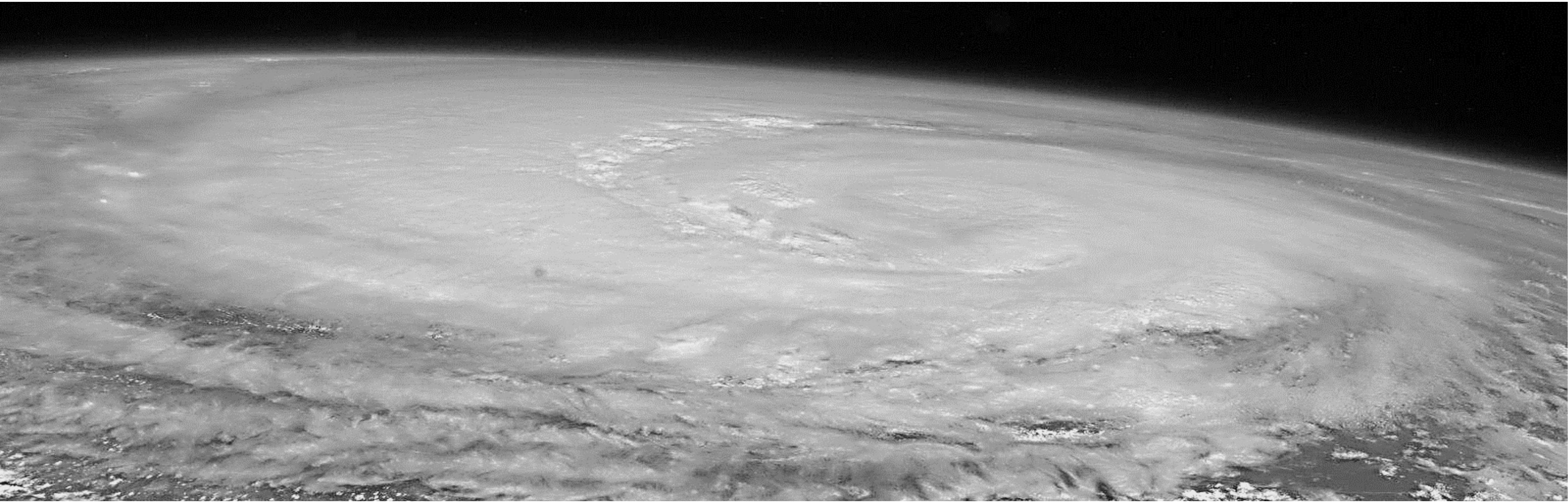
Cloud for DP and DR

Recovery in or from the cloud?

- Recovery from the cloud
    - Measure your recovery performance on prem
    - Understand the best case scenario
    - Test and validate the recover from the cloud
    - Understand the gaps and potential levels of exposure you present with a cloud only recovery strategy
- Recovery in the cloud
    - Cloud to cloud recovery?
    - Within the same cloud recovery?
    - SLAs of cloud provider
    - Commit to testing and validating the recovery process with each and every change.

Disaster Recovery protects from not only physical disasters, but the intangible cyber disasters as well.

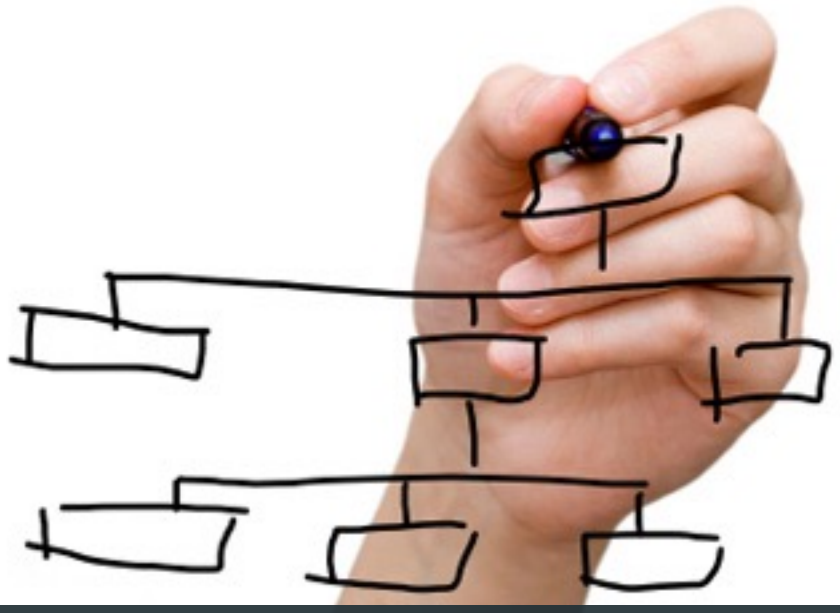
Choosing a Solution



Show your work

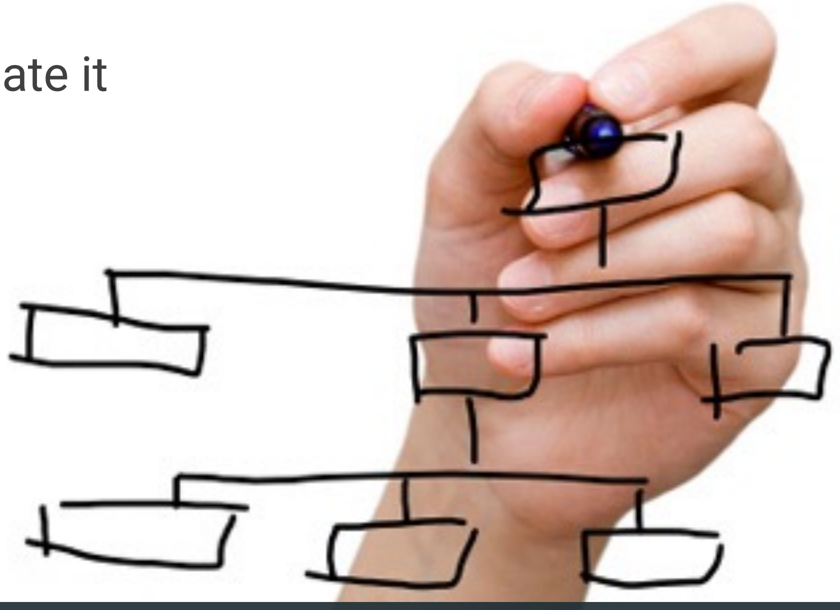
Choosing a Solution

- Solution Selection Criteria
  - Unbiased evaluation of existing solutions based on discovery
    - Hold no biases when selecting a solution for your environment
    - How do each align with your goals, the goals for the business, and recovery requirements?
    - Paper evaluations v Proof of Concept
    - Create the selection and acceptance criteria based solely on your own data points

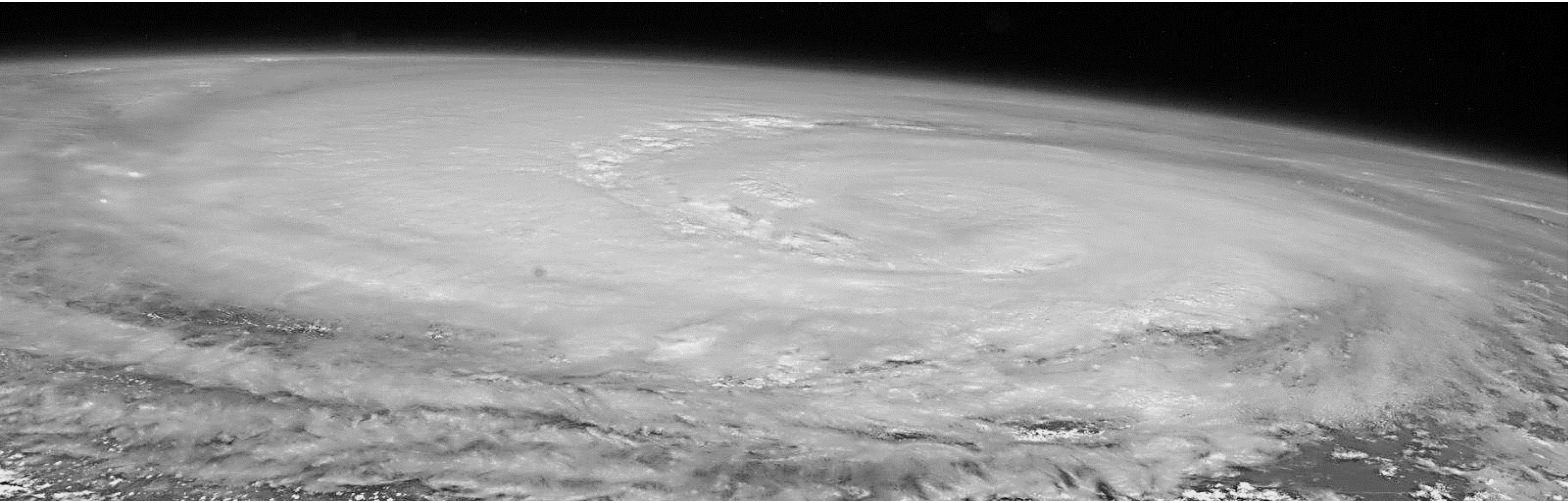


Choosing a Solution

- Solution Selection Criteria
  - Limit the selection pool
    - Create three rounds of evaluation
      - Select 3 to 5 to become part of the short list
      - Reduce down to 2 to 3 for hands on evaluation
      - Thoroughly test based on your requirements
        - Do not let “marketecture” sway you
        - If it isn’t in the current product, don’t evaluate it
        - Be strict with your process



Next Steps: Creating your plan



Final product may resemble a business plan more than a traditional DP/DR plan

The Plan Proposal Outline

- Executive Summary
  - The purpose of the plan
  - Main objectives and goals
  - IT and Business Sponsors
    - Include Key stakeholders
- Business Impact Analysis
  - Identify the risk and associated loss for each business unit
  - What is the continuity strategy
- IT Assessment
  - Capabilities
  - Gaps
  - Strategies
    - Cloud, hot site, cold site, etc.

The Plan Proposal Outline

- Financial Assessment
  - Solution Costs
  - Headcount needs
  - CAPEX/OPEX
  - ROI/TCO
    - Measured based on projected loss from BIA
- Business Continuity
  - Disaster avoidance plans
  - Outline key metrics
    - Time to resolution
    - Customer Satisfaction Rating

The Plan Proposal Outline

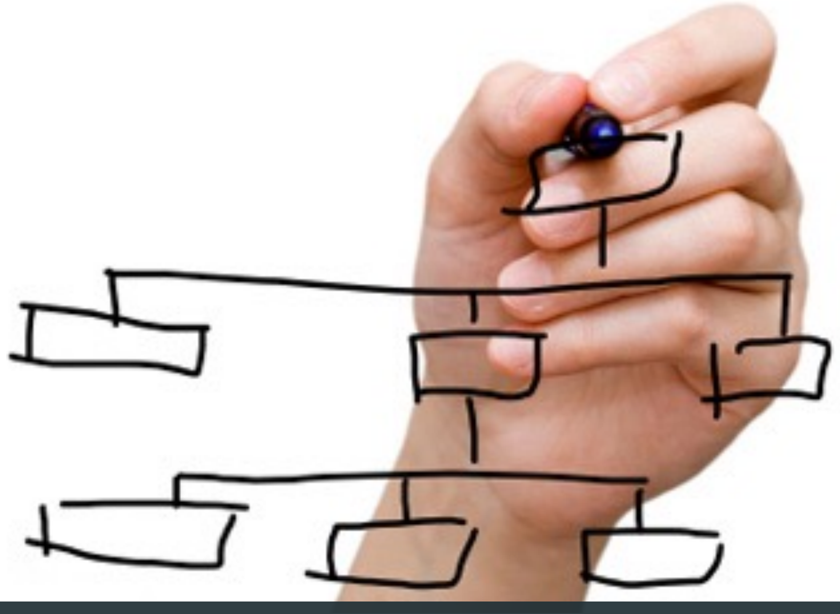
- Recovery Plan
    - Determine Declaration Criteria
    - DR Team
        - Tasks and Responsibilities
        - Call Tree
        - Who can declare disaster?
        - Process for “business as usual”
    - Apps/Systems/Data
        - Business Case
            - Inclusion / Exclusion of specific apps/systems/data

The Plan Proposal Outline

- KPI Section
  - Review cycle, test cycle, audit cycle
  - How all KPIs will be measured
  - Plans for improvement

In closing…

- When Disaster Strikes
  - Be prepared
  - Test regularly
  - Show the results of your tests and corresponding KPI
- Regular meetings with plan sponsors
  - Follow change control management for this plan
  - Get alignment cross functionally
- Money talks
  - Take the details from the BIA and drive that into $$ saved
    - By averting disaster
    - By recovering from disaster
    - By improving business process



5 Key Takeaways

Know the business of the business

Set up regular cross functional team meetings

Teach the business of IT

Get non-IT professionals more engaged

Audit/Review/Test

Absolutes for a solid Business Impact and Recovery Plan

Metrics speak volumes to the business

Use this as a platform to show the value of the plan and execution

Create strategic criteria for workload/workflows

Cloud v. On Premise