
PUG
CHALLENGE
EXCHANGE
AMERICAS
So You've Had a Disaster Now What?
Michael Solomon
June 2016

Agenda

- Where do I even start?
- What's really important?
- What does "recovery" really mean?
- How do I get there?

What is a disaster?

- Unplanned interruption of normal business

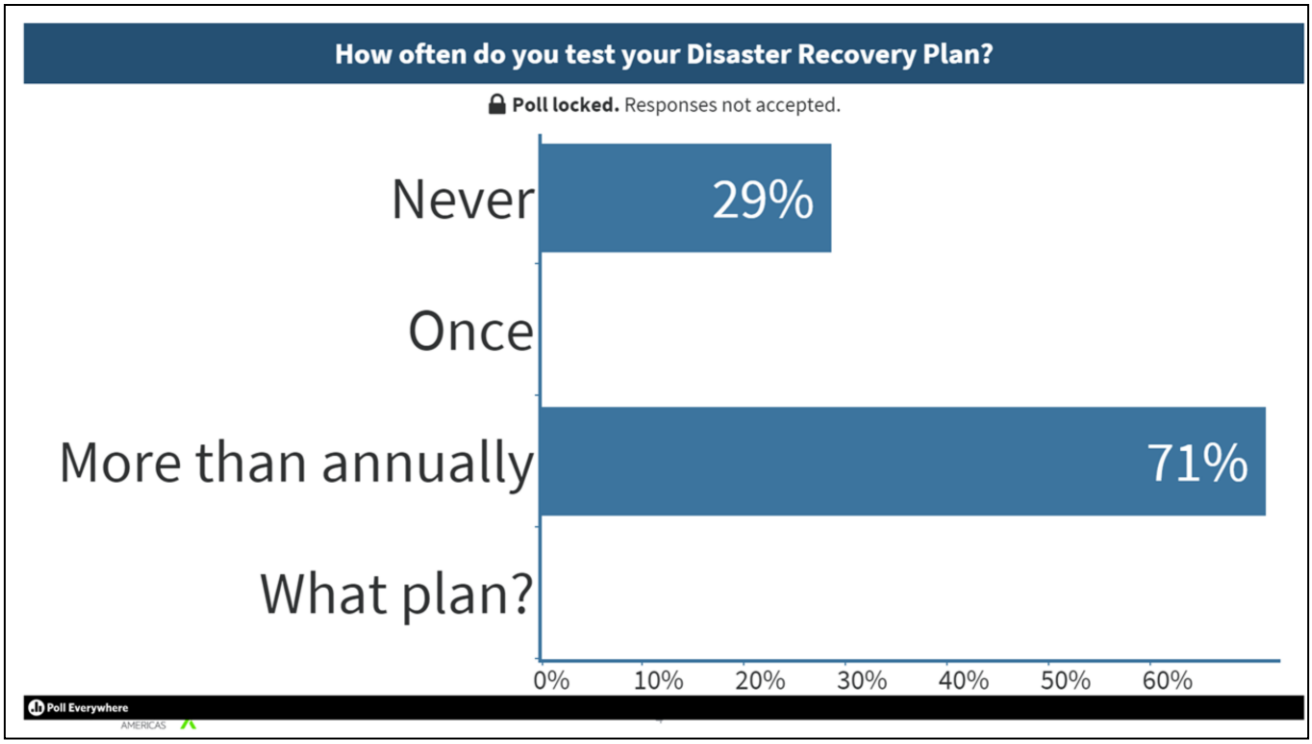
This can be a HUGE topic

- We're just covering the basics today

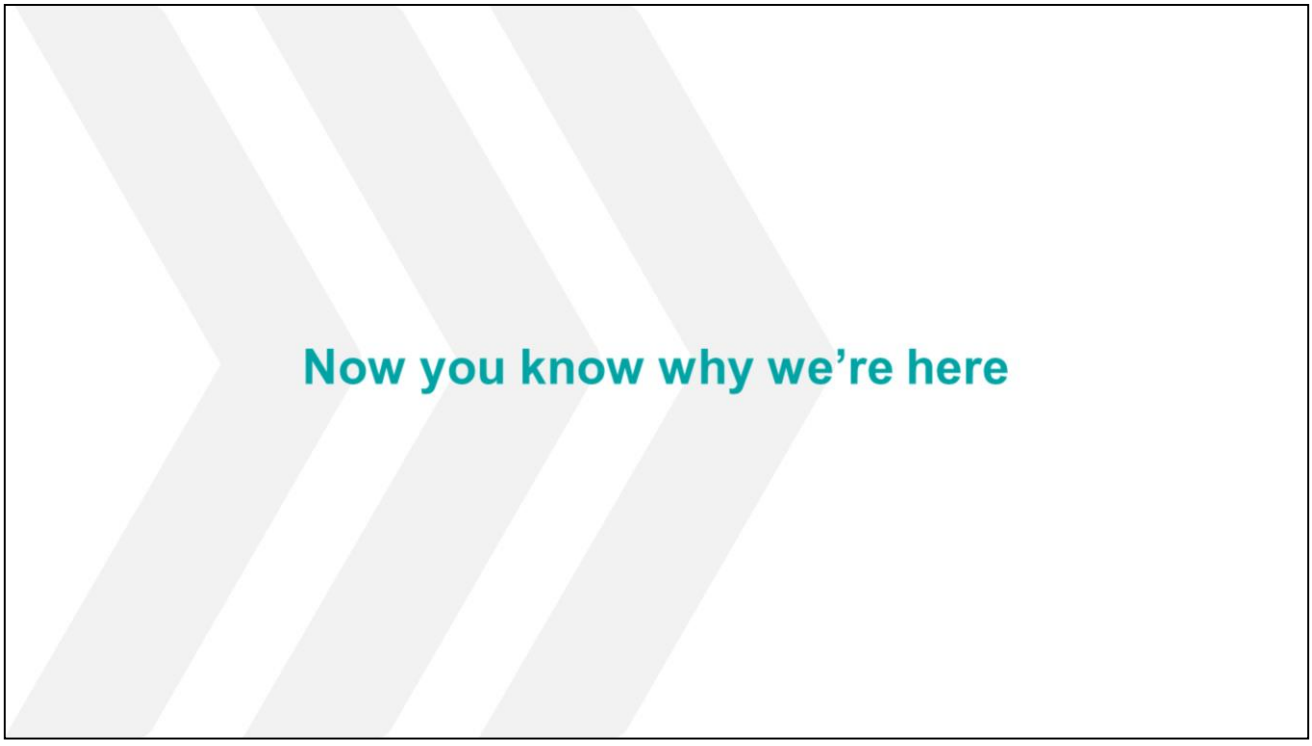
You've heard it all before

- Planning is important

OK, so ...



Results of a live poll of attendees of the talk during PUG Challenge 2016

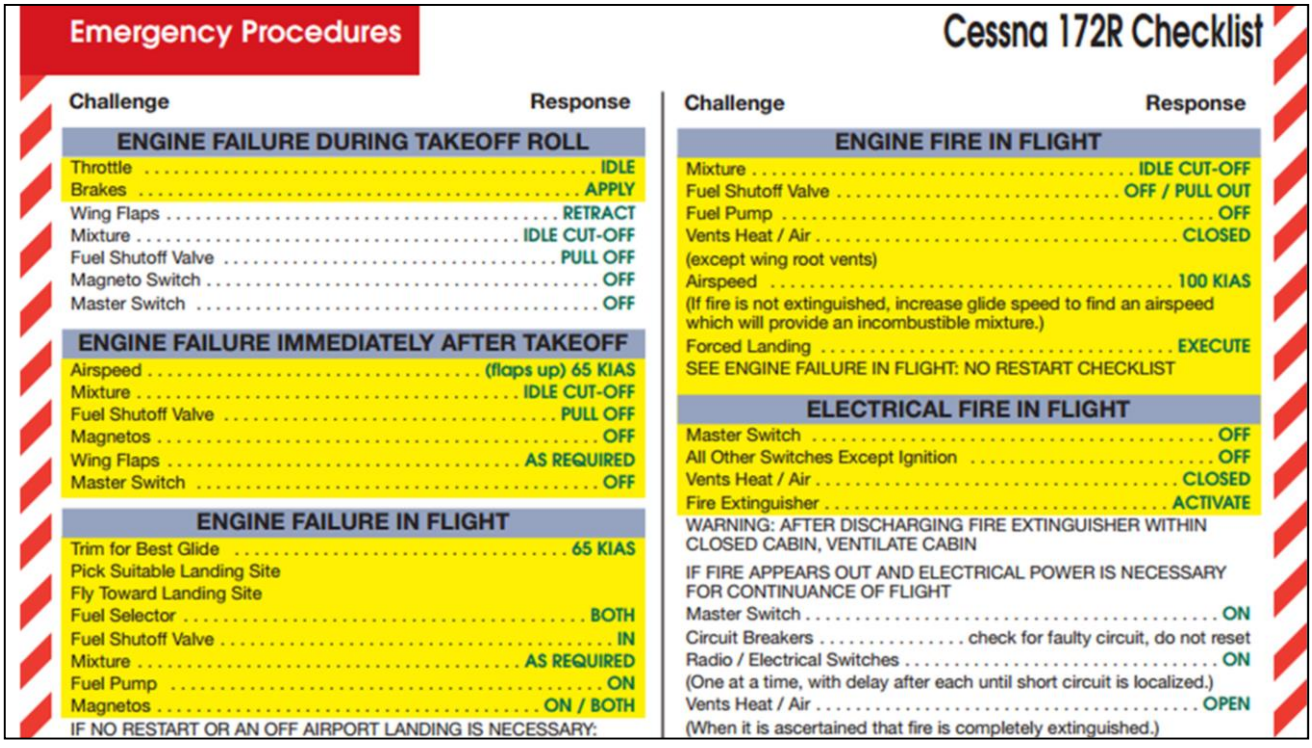

Now you know why we’re here


Disaster recovery is all about
minimizing surprise and
confusion.

Cessna 172 cockpit. What do you do if the engine quits right after takeoff?

(Rotate 55 KIAS, climb 70-80 KIAS)

1) Aviate
2) Navigate
3) Communicate



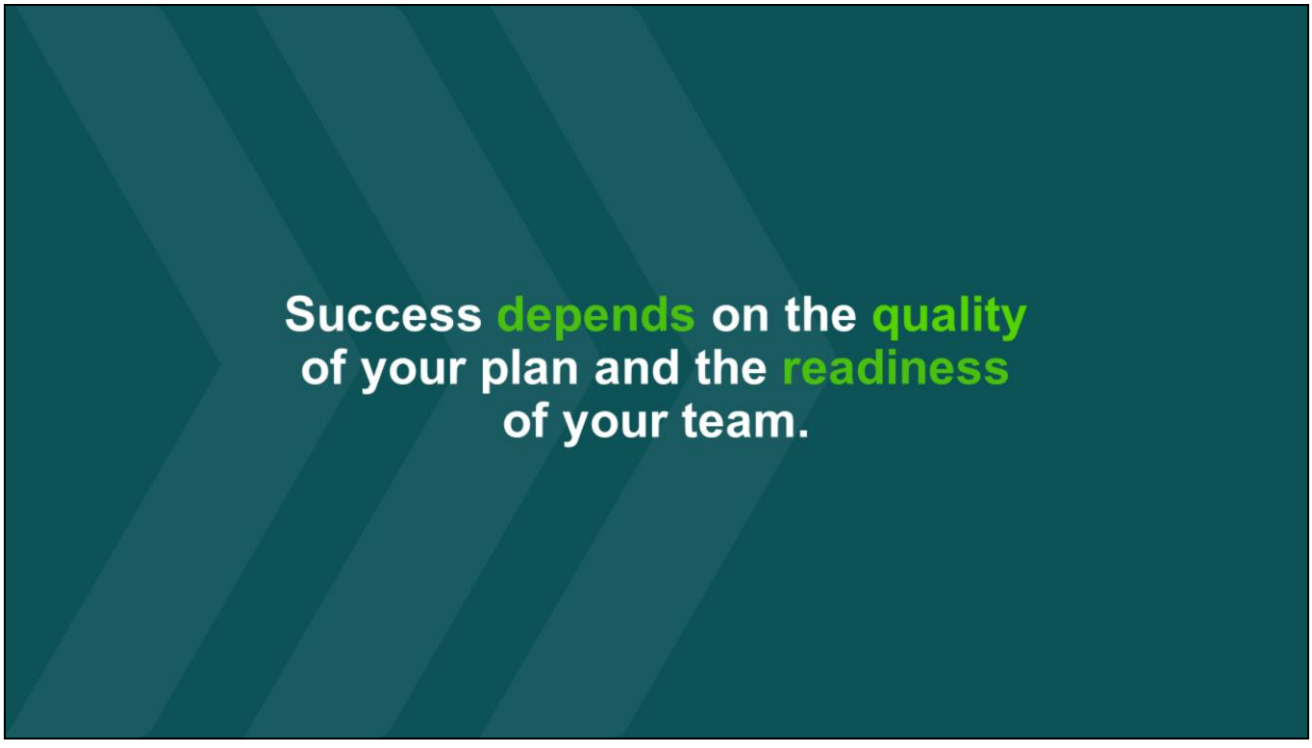
Emergency Procedures

Cessna 172R Checklist

Challenge	Response
ENGINE FAILURE DURING TAKEOFF ROLL	
Throttle	IDLE
Brakes	APPLY
Wing Flaps	RETRACT
Mixture	IDLE CUT-OFF
Fuel Shutoff Valve	PULL OFF
Magneto Switch	OFF
Master Switch	OFF
ENGINE FAILURE IMMEDIATELY AFTER TAKEOFF	
Airspeed	(flaps up) 65 KIAS
Mixture	IDLE CUT-OFF
Fuel Shutoff Valve	PULL OFF
Magnetos	OFF
Wing Flaps	AS REQUIRED
Master Switch	OFF
ENGINE FAILURE IN FLIGHT	
Trim for Best Glide	65 KIAS
Pick Suitable Landing Site	
Fly Toward Landing Site	
Fuel Selector	BOTH
Fuel Shutoff Valve	IN
Mixture	AS REQUIRED
Fuel Pump	ON
Magnetos	ON / BOTH
IF NO RESTART OR AN OFF AIRPORT LANDING IS NECESSARY:	

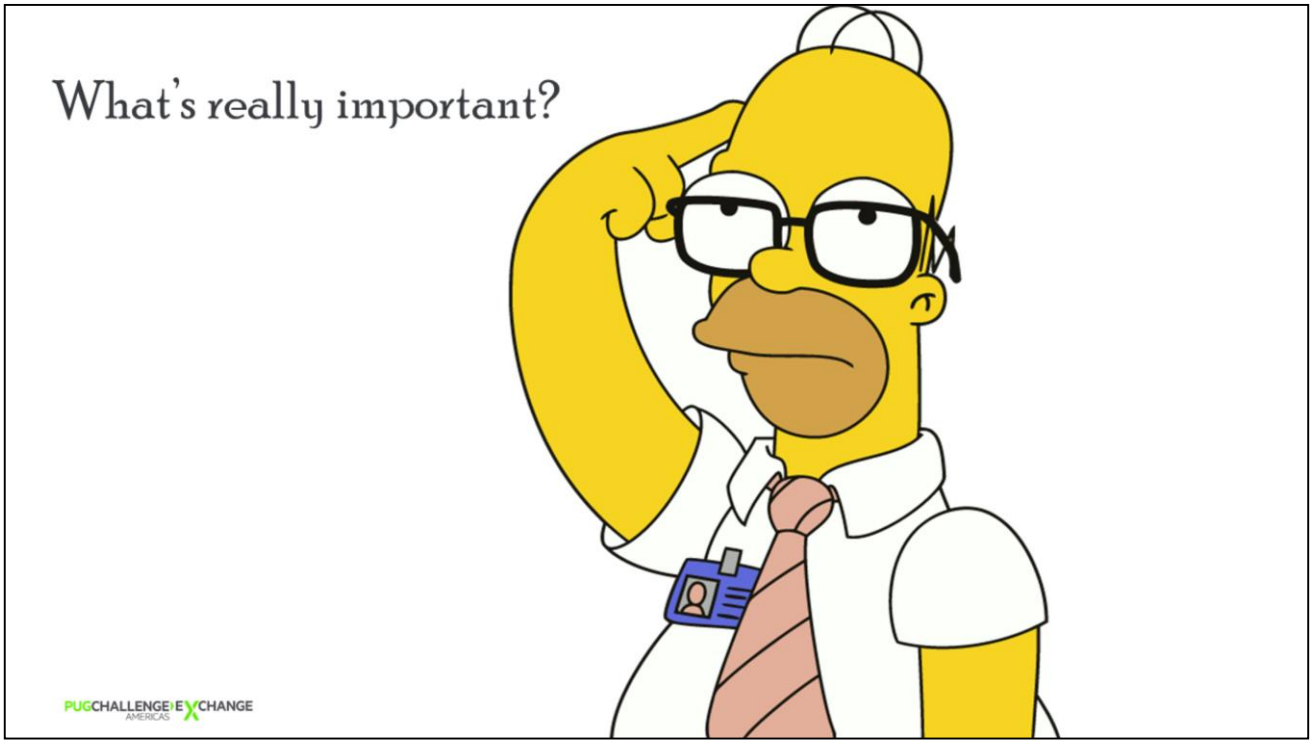
Challenge	Response
ENGINE FIRE IN FLIGHT	
Mixture	IDLE CUT-OFF
Fuel Shutoff Valve	OFF / PULL OUT
Fuel Pump	OFF
Vents Heat / Air	CLOSED
(except wing root vents)	
Airspeed	100 KIAS
(If fire is not extinguished, increase glide speed to find an airspeed which will provide an incombustible mixture.)	
Forced Landing	EXECUTE
SEE ENGINE FAILURE IN FLIGHT: NO RESTART CHECKLIST	
ELECTRICAL FIRE IN FLIGHT	
Master Switch	OFF
All Other Switches Except Ignition	OFF
Vents Heat / Air	CLOSED
Fire Extinguisher	ACTIVATE
WARNING: AFTER DISCHARGING FIRE EXTINGUISHER WITHIN CLOSED CABIN, VENTILATE CABIN	
IF FIRE APPEARS OUT AND ELECTRICAL POWER IS NECESSARY FOR CONTINUANCE OF FLIGHT	
Master Switch	ON
Circuit Breakers	check for faulty circuit, do not reset
Radio / Electrical Switches	ON
(One at a time, with delay after each until short circuit is localized.)	
Vents Heat / Air	OPEN
(When it is ascertained that fire is completely extinguished.)	

Specific steps for handling engine failure in different flight regimes.



Medical emergency (someone has to take the lead):

A. Assign someone to call 911/go for help
B. B. Send someone else for a first aid kit/supplies
C. C. Assess situation
D. D. Render aid



Think it through

- Before the disaster
- What do you really need for operations?
  - Low tech alternatives may be fine

Write it down

- The only way to retain and communicate
- What if you aren’t available?

Prioritize

- You can’t do everything
- Avoid wasting time

- Recovery - The point at which you can carry on
- Restore ≠ Recovery
  - *prorest* isn't enough
  - More than just backups (or even replicated databases)

PUGCHALLENGE EXCHANGE AMERICAS

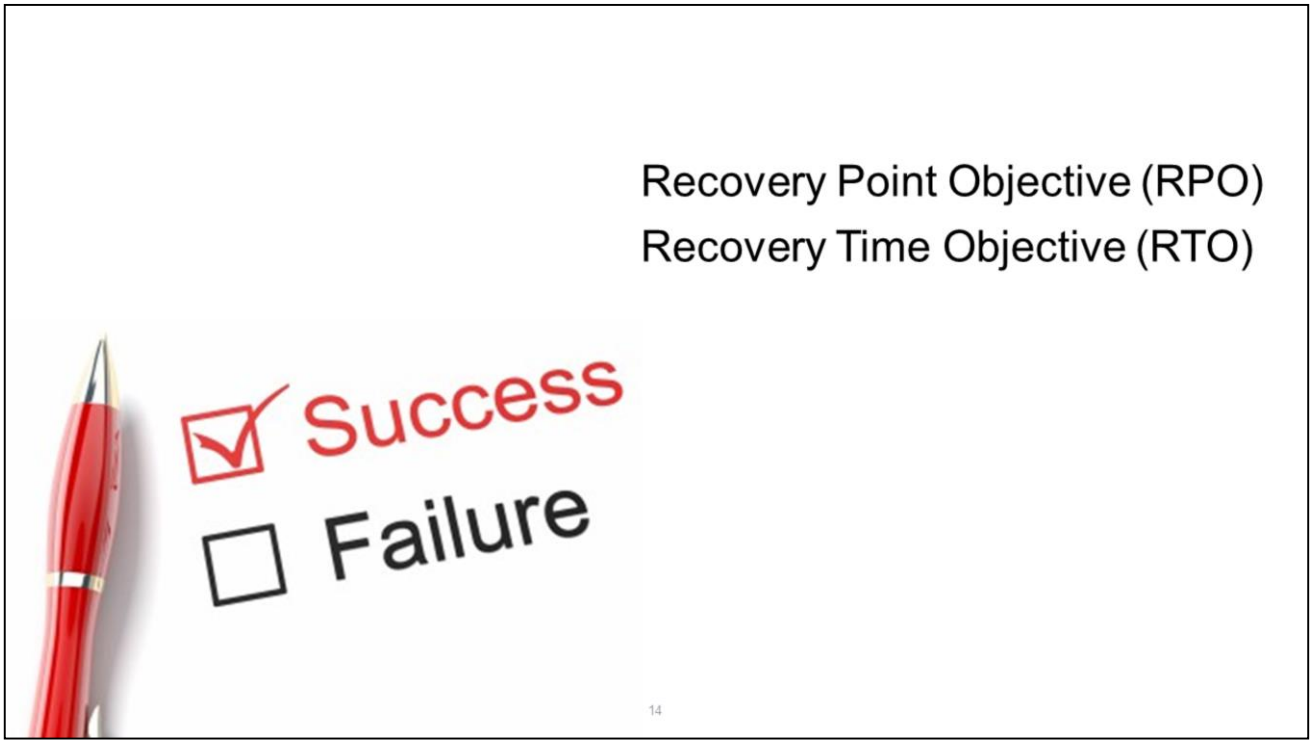
13

The point at which you can carry on

Recovery Point Objective (RPO)

How long to get there?

Recovery Time Objective (RTO)



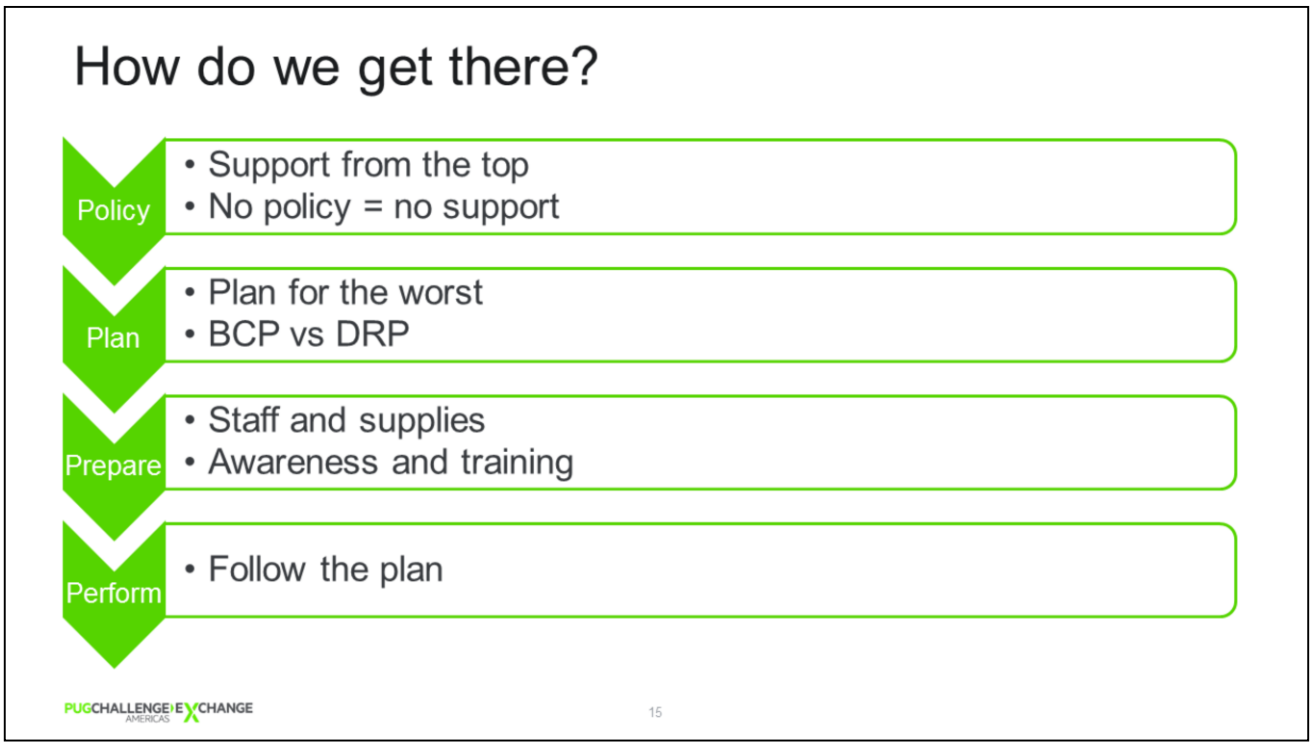
Recovery Point Objective (RPO)

How long to get there?

Recovery Time Objective (RTO)

RPO and RTO defined by business

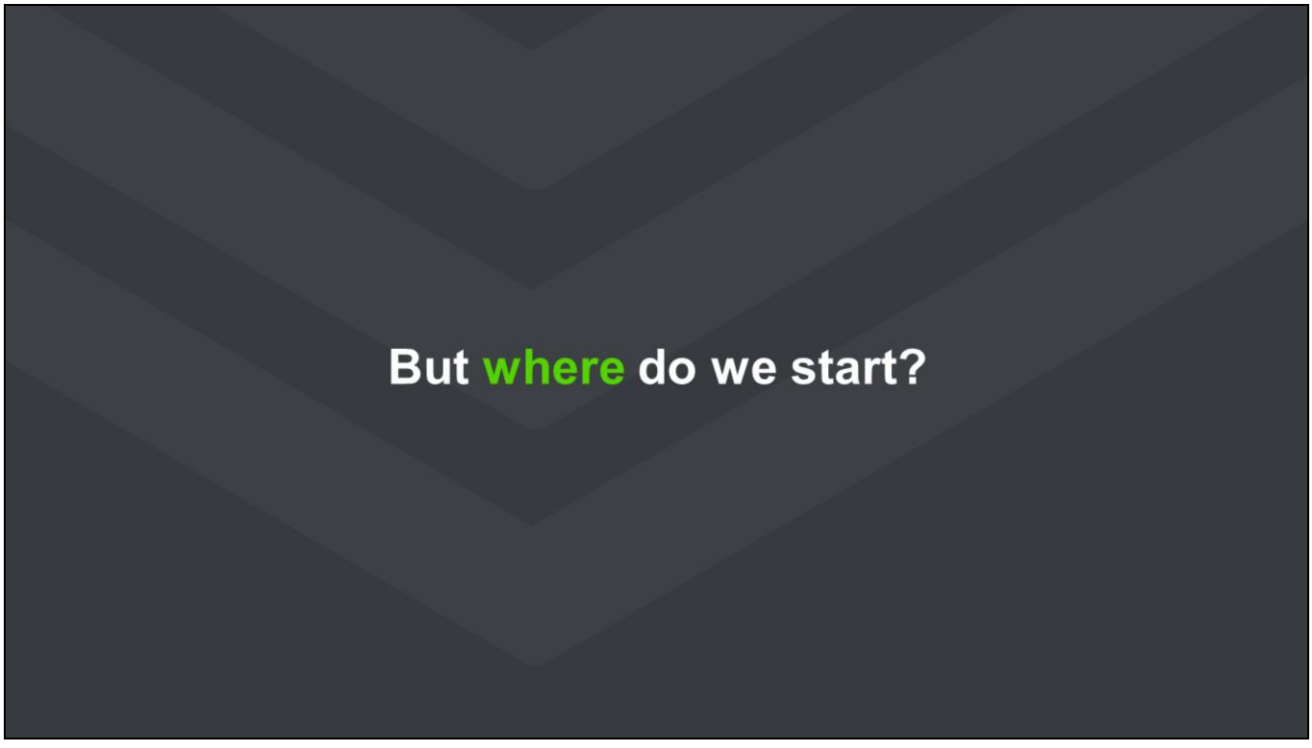
Not IT



BCP vs DRP

DRP recovers data and infrastructure (short term)

BCP restores business process (long term)



That’s all great, but how do we develop a plan?

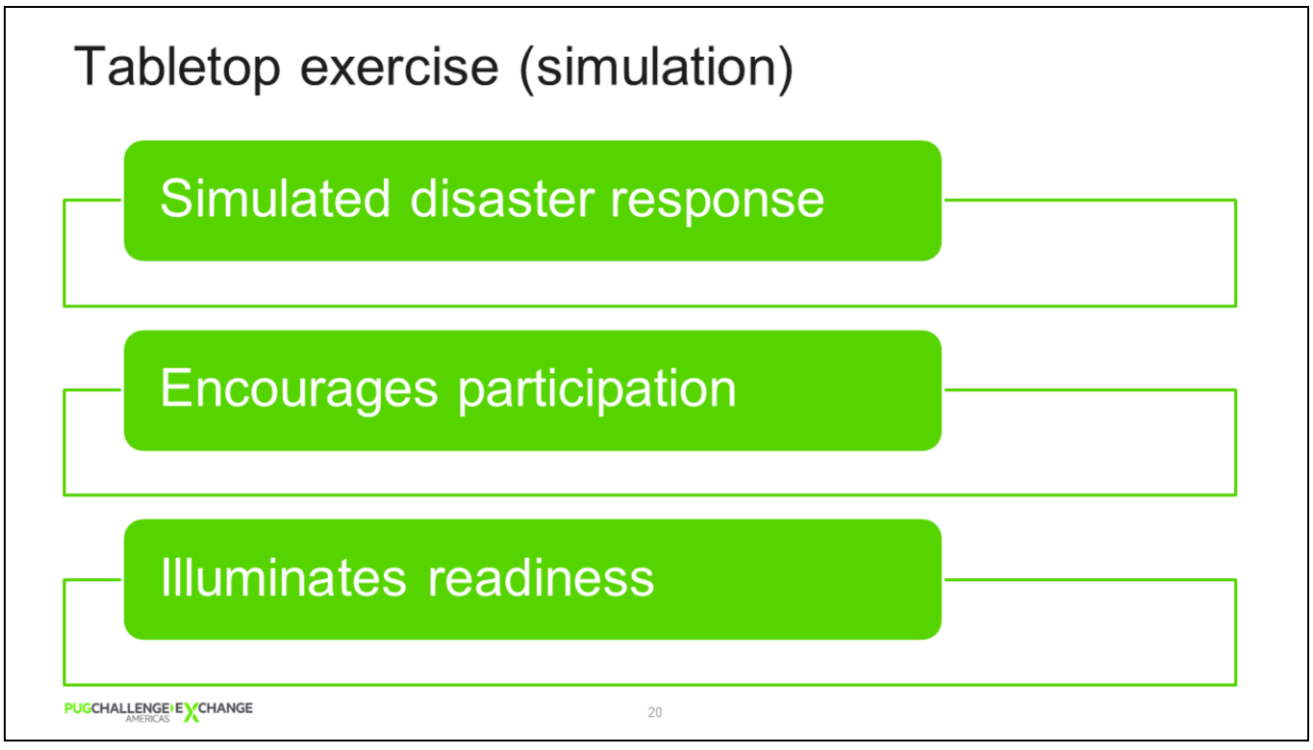
Gamification

RPG

LARP

OK, not that type of RPG!

This is a picture of a real Tabletop Exercise (simulation)

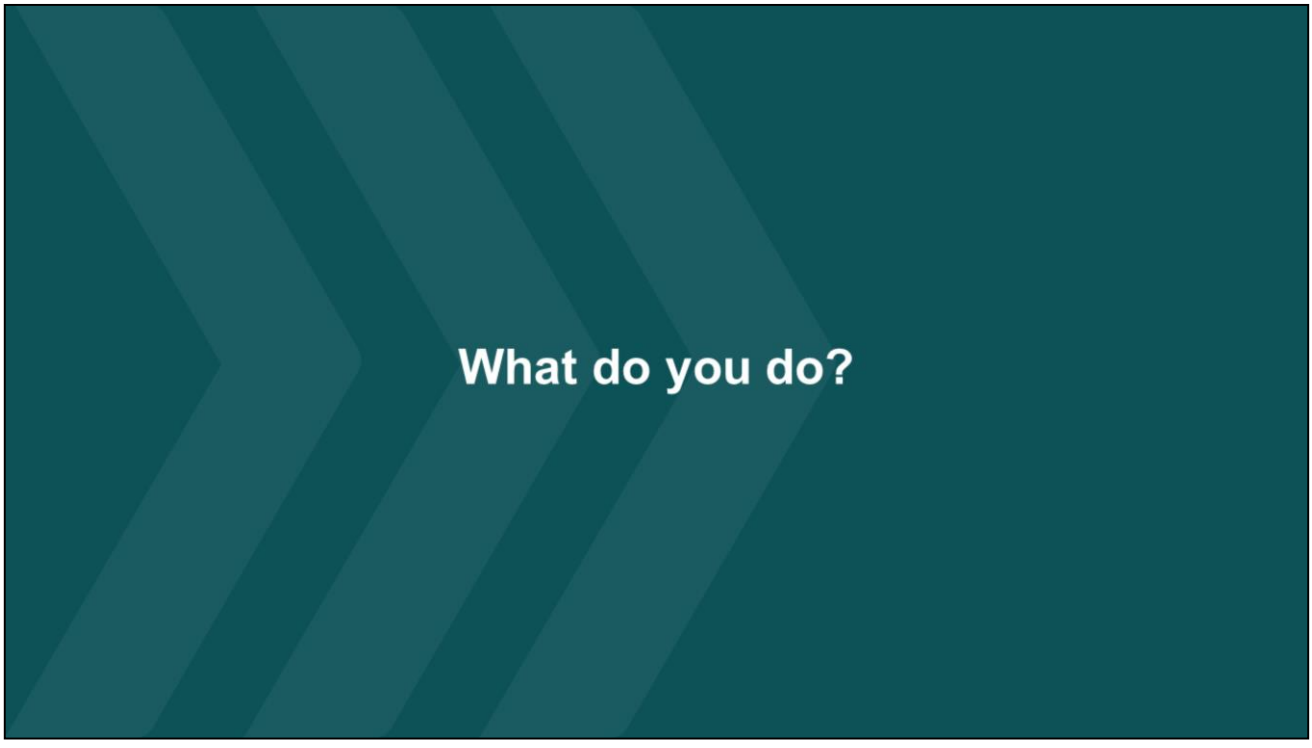


Walkthrough your plan (OR see how hard it is to “make it up as you go” if you don’t have a plan)

Example challenge scenario (segment 1)

- Small fire just outside the data center, setting off the alarm system
- Sprinkler extinguishes the fire by the time the fire department arrives
- The building has been evacuated
- Personnel and the media are aware of what happened
- Then, as people begin to go back inside
  - The receptionist takes a call from someone who indicates that the fire is "only the beginning" because the company hasn't treated him right

http://www.csoonline.com/article/2120836/disaster-recovery/pandemic-preparedness-tabletop-exercises-three-sample-scenarios.html?upd=1466709319099



Let the audience make suggestions.

Tips:

1) Who does the receptionist call?
2) When does HR get involved?
3) Who answers media questions?
4) Should you call LE? Who calls? Who do you call?
5) Do you let employees back into to building?

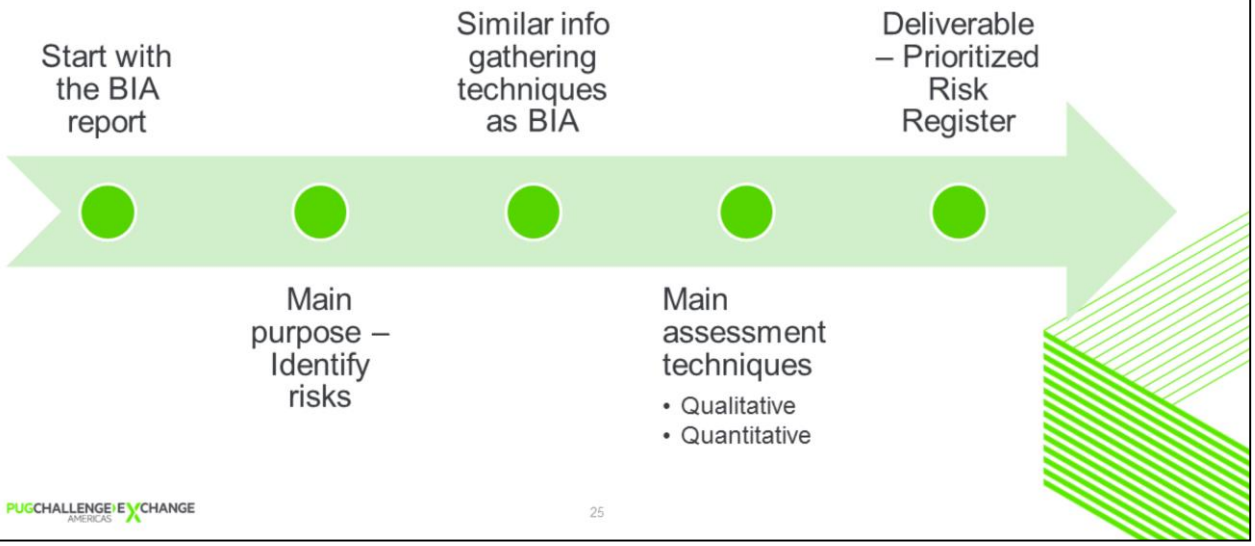
DRP Planning steps

Business Impact Analysis (BIA)	• Identify critical business functions • Identify risks
Prioritize	• Risk value • Cost of remediation
Select Controls	• Preventative / Detective / Corrective / Compensating • Use multiple types
Document	• Clear and succinct • General target audience
Test	• Tabletop exercises • Escalating reality tests

Business Impact Analysis - BIA

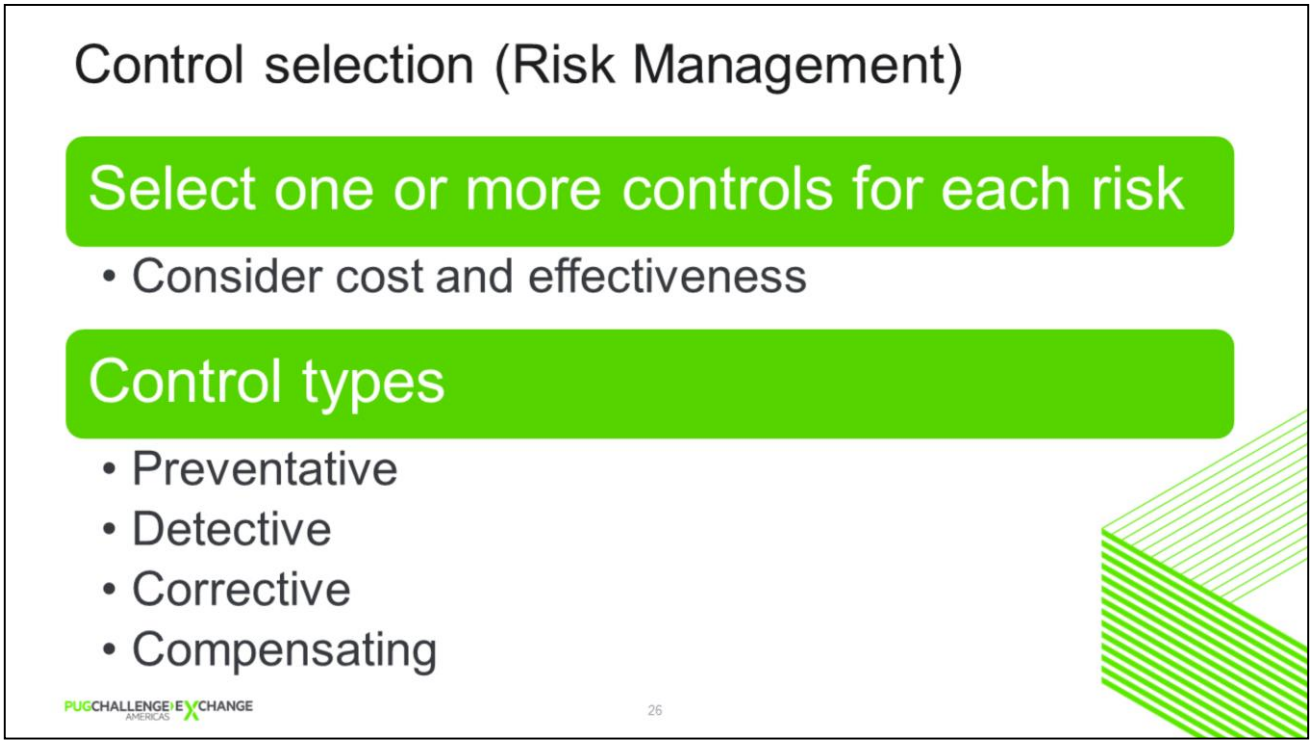
Identify each critical business functions	• Must have upper management support • What functions are critical to the business (not IT)?
Consider disruption impact	• Lost/delayed revenue / Increased expenses • Fines/penalties / Reputation
Timing and duration	• Does disaster timing matter? • How long can you be down?
Methods	• Questionnaire • Focus group • Interview

Risk Assessment

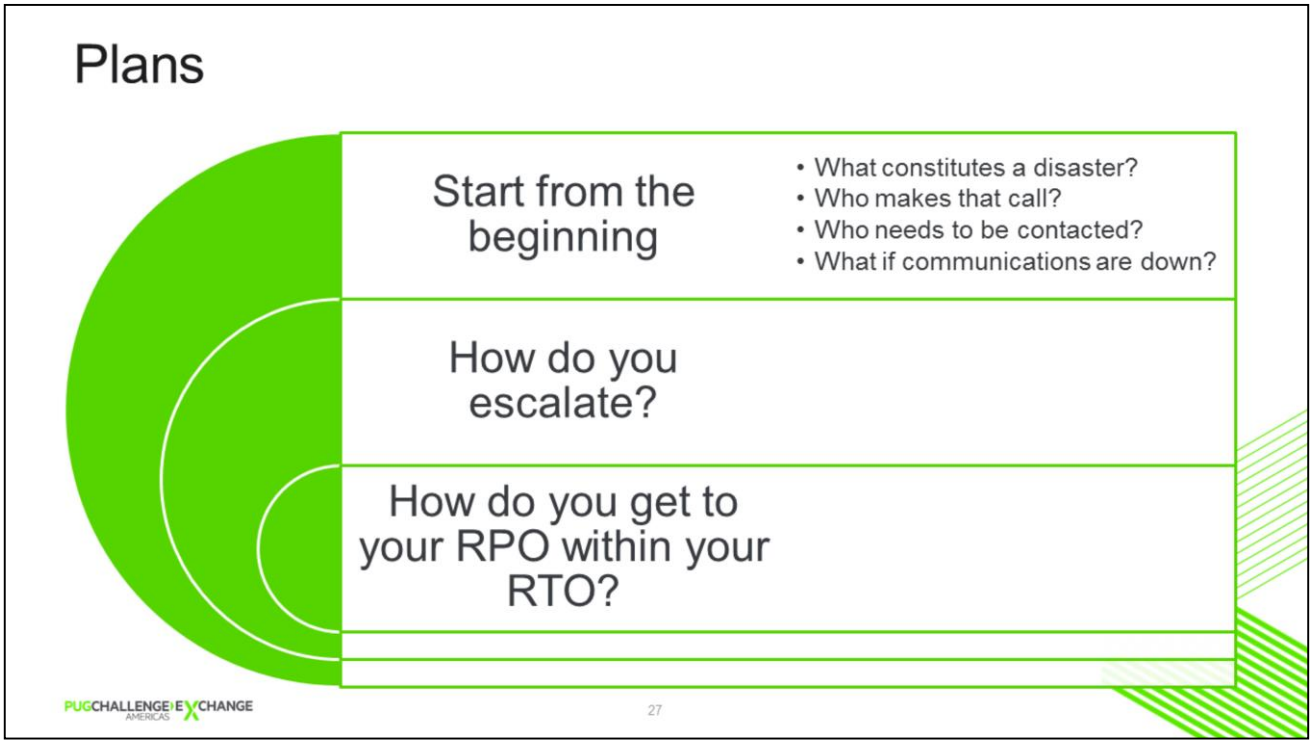


PUGCHALLENGE EXCHANGE AMERICAS

25



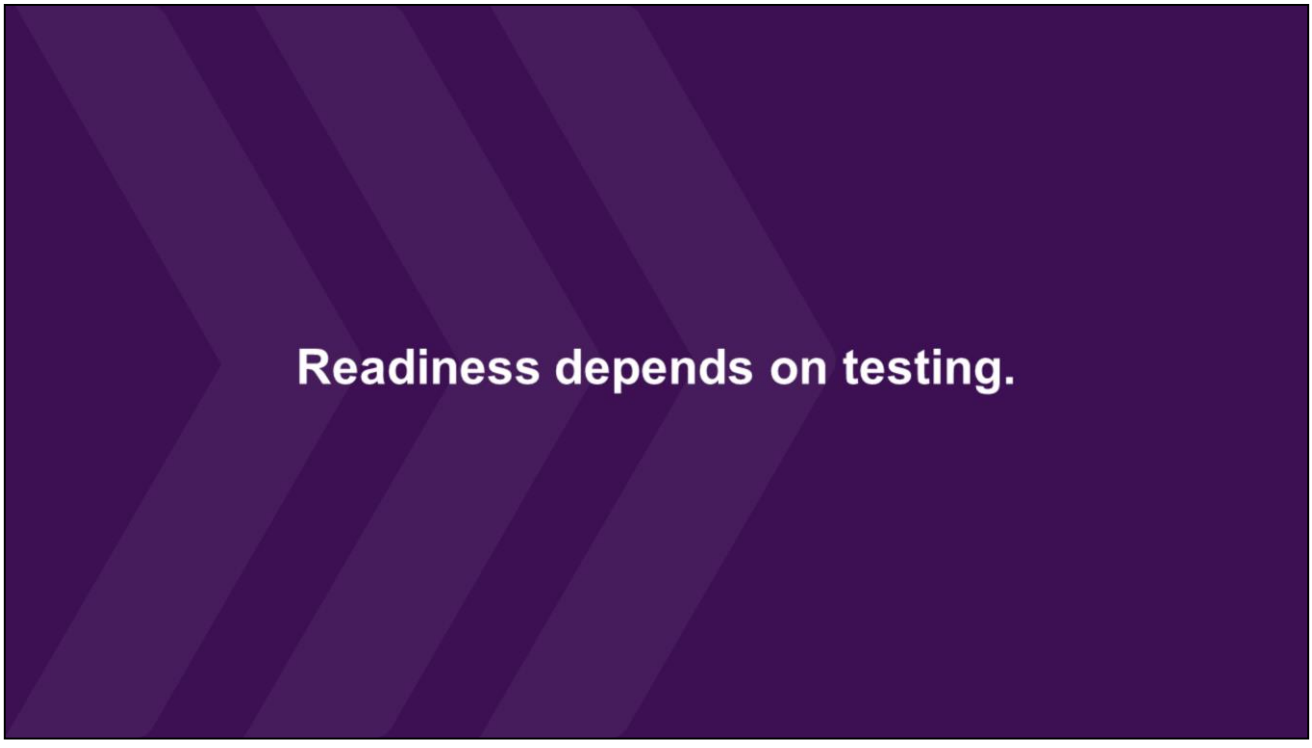
Best way to handle disasters: Avoid them!



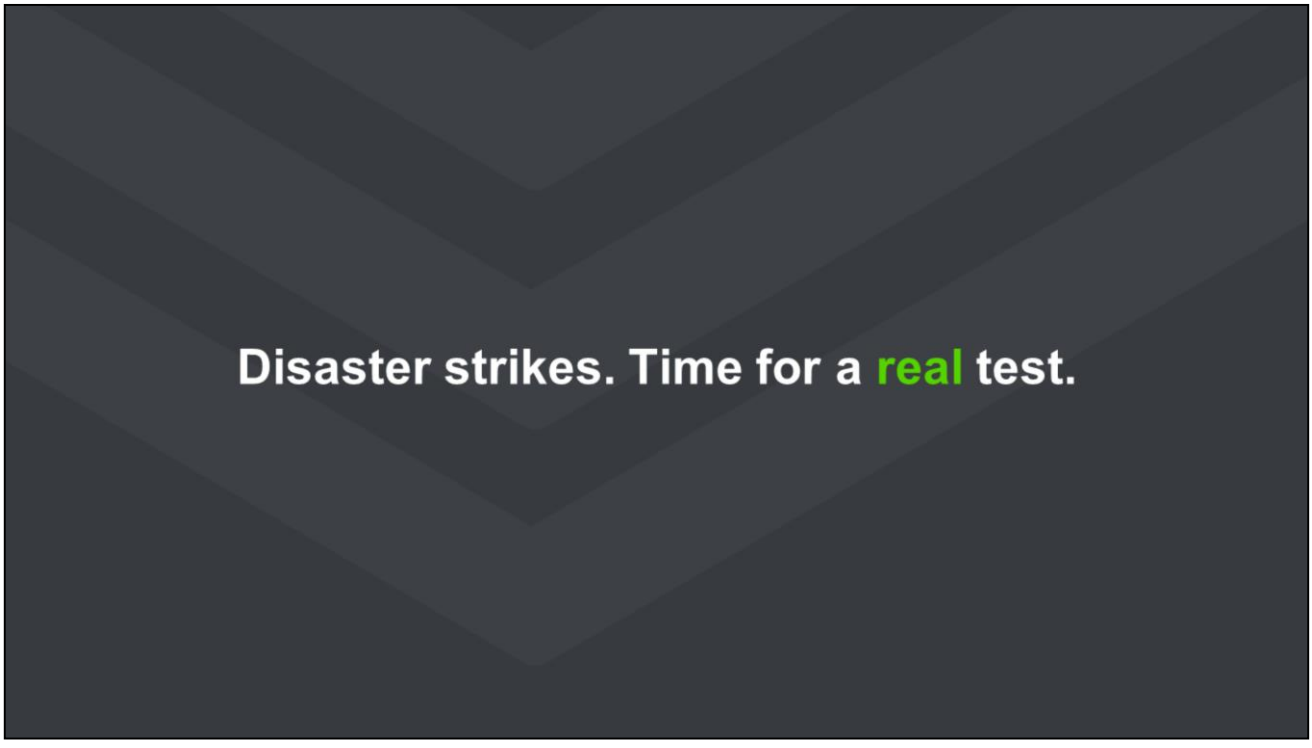
http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-management/business-continuity-plan-development.aspx

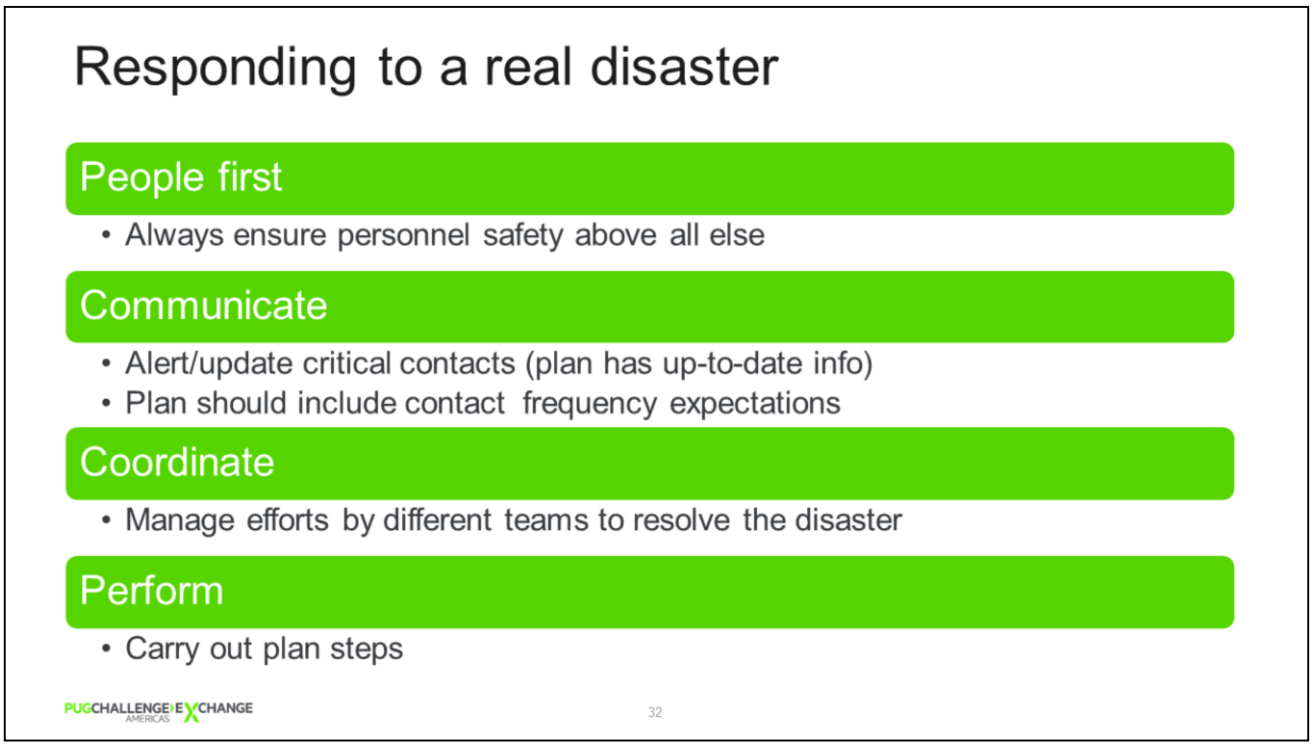
How can I mess this up?

- Sloppy BIA
- Focus on technology
  - Planning and solutions
- Process too complex
- Lack of
  - Testing
  - Maintenance (configuration drift)
  - Awareness/training

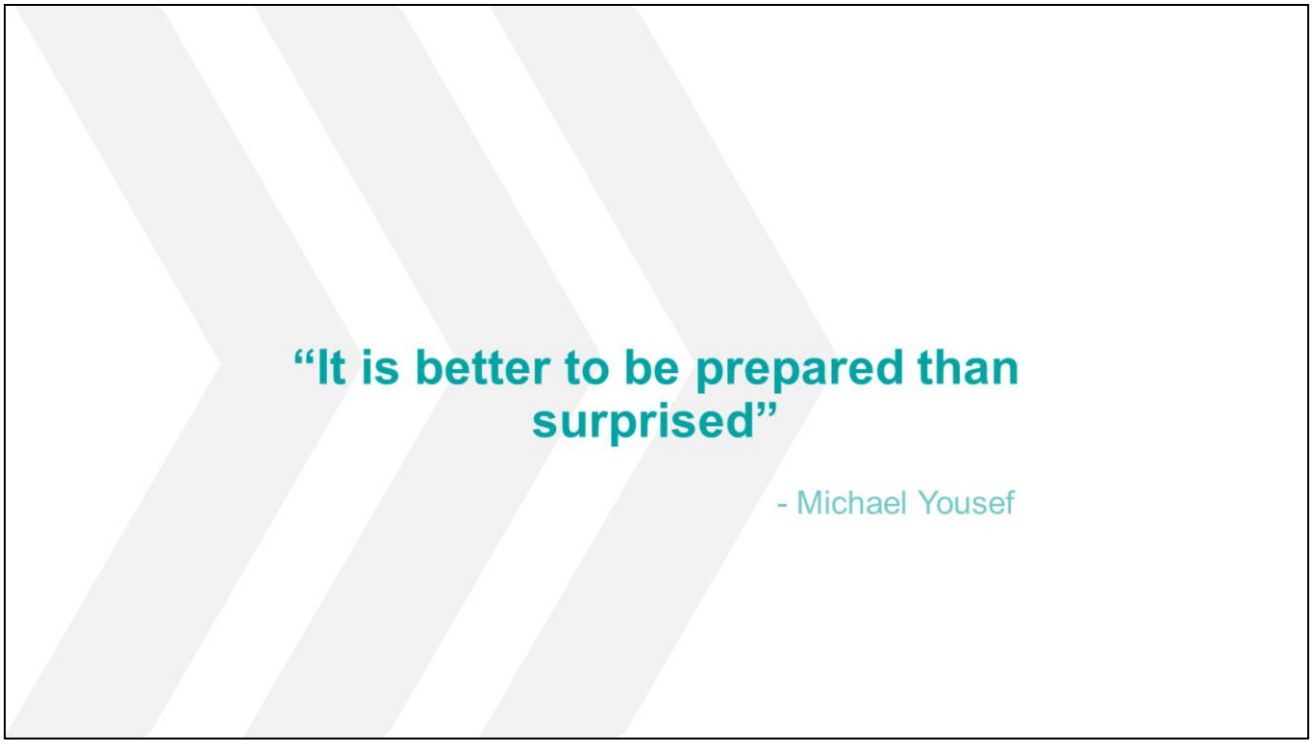

Readiness depends on testing.

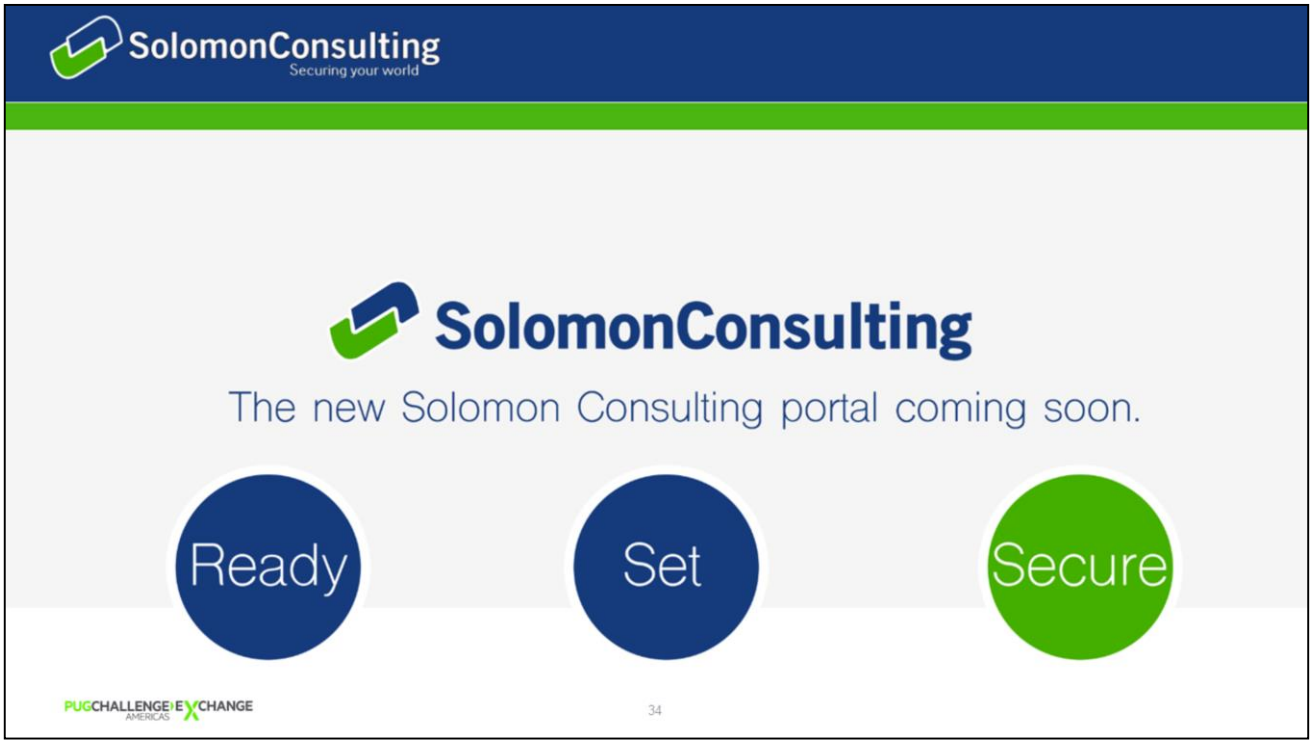
As you move down the list, risk increases. Only execute a cutover test if mandated or if you’ve been through the other tests successfully!


Disaster strikes. Time for a real test.



1. Protect people first!
2. Communicate- Ops/Mgmt/HR/PR/Utilities/Vendors/Agencies/LE- Know contact info (and specific names)- What if phones/cell service is out?
3. Coordinate- Who's responsibility is this?- SLA, etc.- What needs to be recovered? (service/hardware/software)
4. 4. Make the call and follow the plan


“It is better to be prepared than surprised”
- Michael Yousef



www.solomonconsulting.com

Resources

- NIST SP 800-34 “Contingency Guide for Information Technology Systems”
- ISO 17799
- COBIT
- DRI International (https://www.drii.org/)
- http://searchdisasterrecovery.techtarget.com/feature/Using-a-business-impact-analysis-BIA-template-A-free-BIA-template-and-guide
- Michael Solomon (michael@solomonconsulting.com)
- http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/business-continuity-planning-process.aspx
- http://www.csoonline.com/article/2120836/disaster-recovery/pandemic-preparedness-tabletop-exercises-three-sample-scenarios.html?upd=1466709319099
- http://www.csoonline.com/article/2132392/supply-chain-security/3-more-tabletop-exercises-for-business-continuity.html