Developing and Conducting a Table Top Exercise

Vicky McKim, AFBCI, MBCP, CRMP

///AUREON™

Humor or Reality?

Session Overview

- Different Types of Exercises
- Preparations for an Exercise
- Monitor Findings Resolution
- Incorporating Exercising into Your Risk Management Program

Types of Exercises

- Purpose
- Value

- Table Top
- Walk Through
- Simulation
- Test
- Full Recovery Exercise

Table Top

Table Top

- Primary purpose is to familiarize teams with the recovery process
- Review the details of their recovery plan
- Frequent table tops help keep teams ready to respond
- Level 1 of stress inoculation

Walk Through

Walk Through

- Primary purpose is to verify the recovery process actions with multiple groups at once
- Helps uncover plan gaps
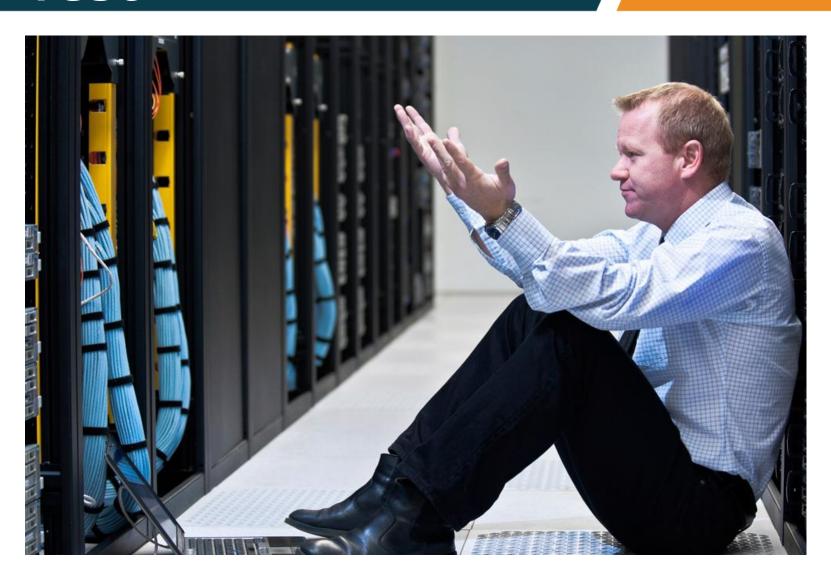- Dependencies are highlighted
- Level 2 of stress inoculation

Simulation

Simulation

- Primary purpose is to actually role play through business or IT recovery
- Conduct briefings, allow team work time and issue resolution
- Helps eliminate recovery theory
- Communications is usually a key component
- Level 3 of stress inoculation

Test

Test

- Primary purpose is to recover a portion of the processes or technology at an alternate site
- Validates plans work
- Exposes remaining gaps and theory
- Level 4 of stress inoculation

Full Recovery Exercise

Full Recovery Exercise

- Primary purpose is verify how long it takes to recover if everything is down at once
- Usually for the heavily regulated or critical infrastructure/service companies
- You find your pain points for a catastrophic recovery event.
- Level 5 of stress inoculation

Layered Preparation

- Pick a likely threat that has high impact potential
- Exploit plan gaps
- Check dependencies
- Test the theory
- Time it

Tabletop Prep

- Create a scenario related to a high probability and impact threat
- Schedule individual team meetings
- Bring their continuity plans
- Read the scenario and talk it through
- Each team will check to see if their plan addresses steps needed for response

Walk Through

- Add a few teams
- Focus on validating dependency requirements
- Are the dependencies accounted for in the plans
- Document the gaps as findings
- Assign responsibility for the fix

Simulation

- Serious impact scenario
- Company wide – all the teams
- Role play based on plans
- Injects for realism
- Black list a few key employees
- Focus on communication, issue resolution
- Manage the CHAOS

Test

- Use backups to recover a limited scope of systems/processes at a remote location
- Examples: only accounting systems or call center operations
- Document the technical issues as findings and who has responsibility for resolution

Full Recovery Test

- Recover all systems, services and processes at a remote location
- All critical staff – serious chaos
- Speed is paramount – work to the RTO
- Document the gaps as findings and who has responsibility for resolution
- Very few companies ever do this type

Findings

- What is it
- Who can fix it
- When is it due
- What is the final resolution
- Is it documented
- Close the finding

Managing to Your Program

- Incorporate participation and findings resolution as internal audit measurement
- Log participation - dates for external audit
- Executive participation critical to program success
- Report summary results to executives
- Publish detailed results for team leaders and managers – fosters improvement

Take-Aways

- Start with a simple one
- Use probable threats to make it real
- Use injects
- Let findings be the indicator for next level