CREATING AND RUNNING AN IT DISASTER RECOVERY TEST

Ray Holloman, M.S, M.B.A, CBCP

1

ABOUT ME

- 6 years in Business Continuity/Disaster Recovery
- 10+ years in the IT/Healthcare Industry
- Masters in Information Security and Business Administration
- CBCP Certified
- Assisted or Managed over 30 Full Exercises

2

ABOUT MY PROGRAM

- 4 Full Data Center Exercises per year
- 8 Project Windows Per Year
- Largest Test is over 175 applications
- Smallest test is under 10 application

3

PREPARATION

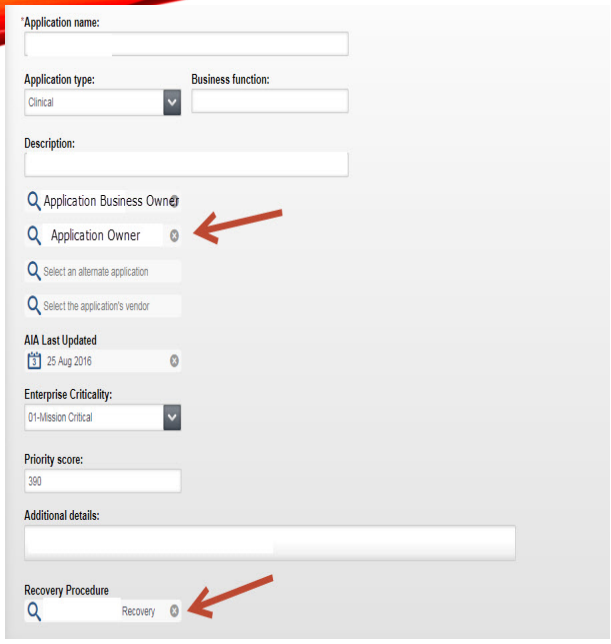
4

HOW OUR PLANS COME TOGETHER

- The Application Dictionary is used to update the Plans and attributes to update the teams.
- As we share this environment with other lines of business, IT does have control over the Application Dictionary.
- Adding fields to the dictionary, allows for reports to be created instead of having to use task and traditional teams.

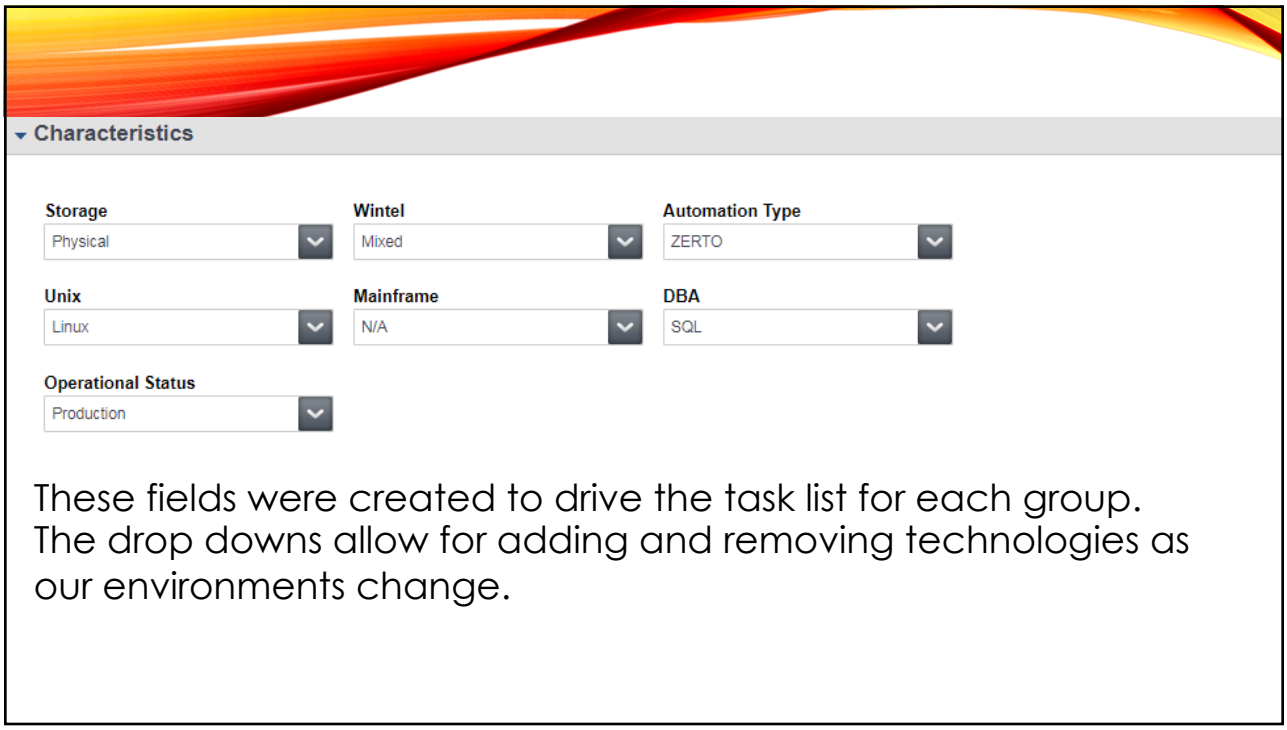
5

Application owner allows for the ability to have them all in one report to contact if something happened to the data center.



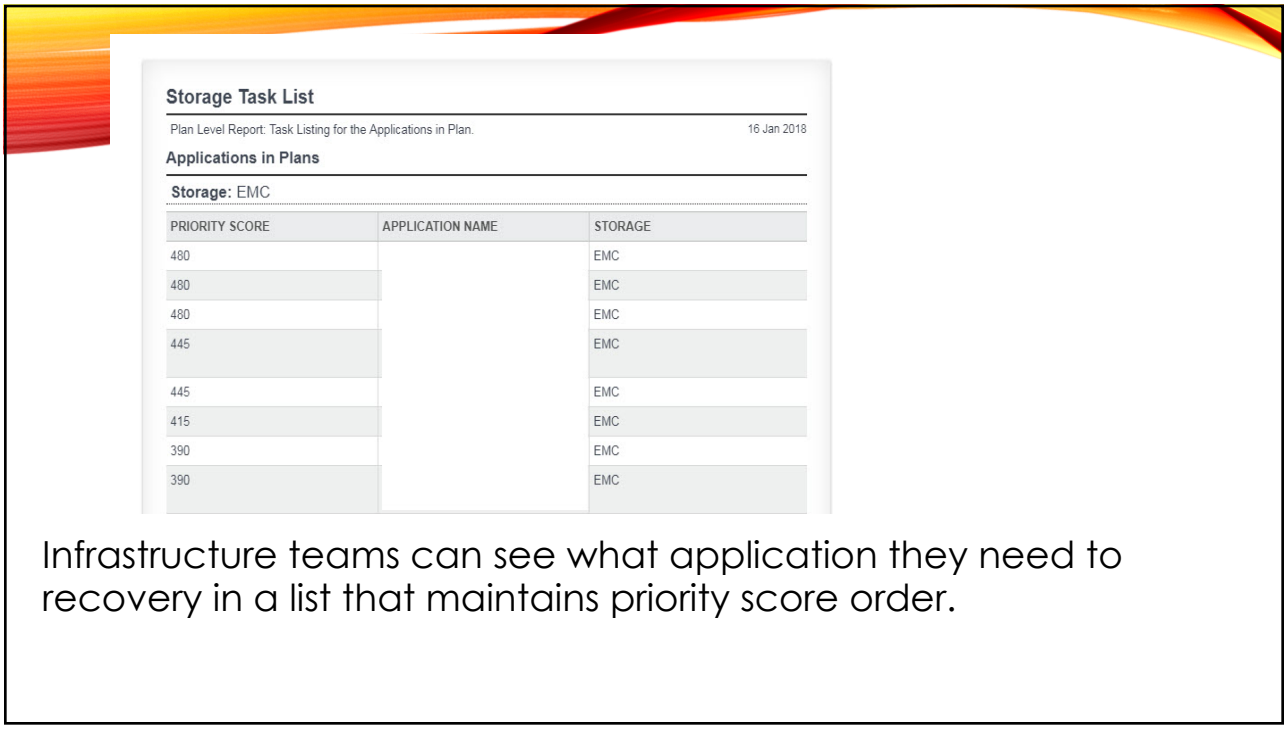
Adding the Recovery Procedure the allowed at the end for tasks to be removed.

6



These fields were created to drive the task list for each group. The drop downs allow for adding and removing technologies as our environments change.

7



Storage Task List

Plan Level Report: Task Listing for the Applications in Plan. 16 Jan 2018

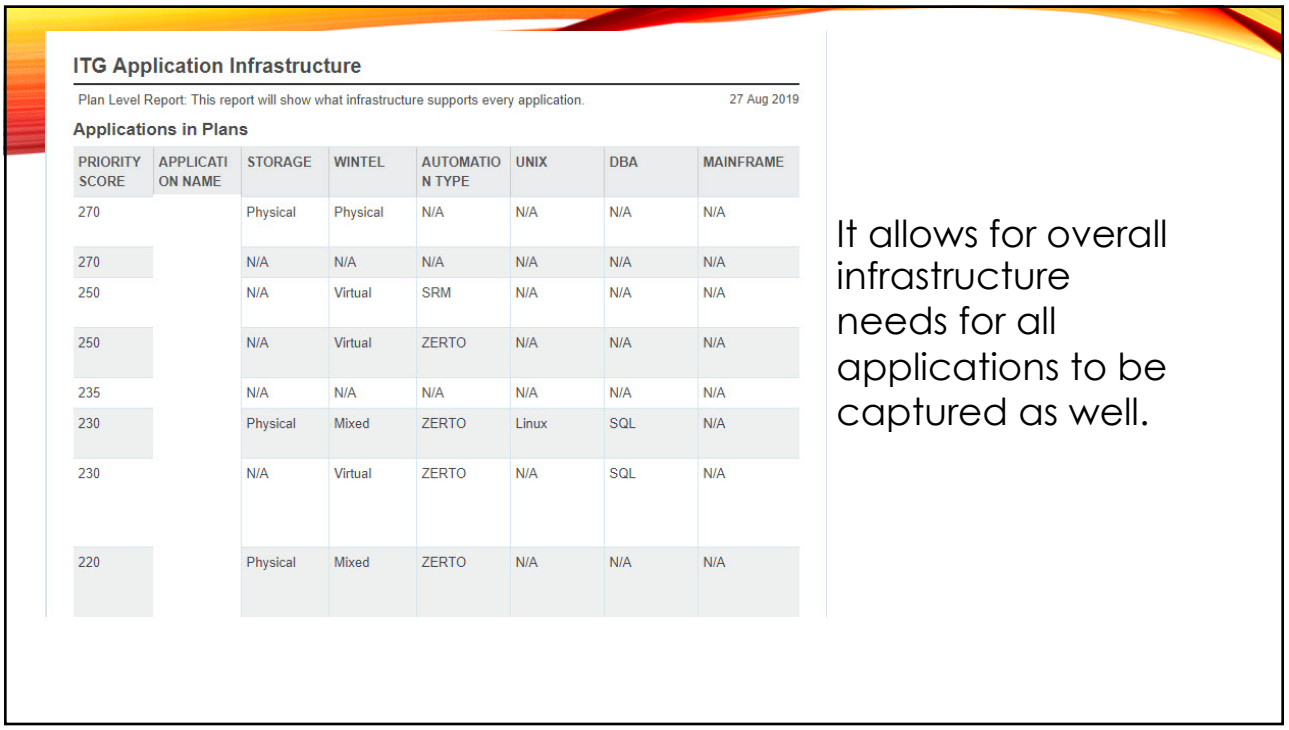
Applications in Plans

Storage: EMC

PRIORITY SCORE	APPLICATION NAME	STORAGE
480		EMC
480		EMC
480		EMC
445		EMC
445		EMC
415		EMC
390		EMC
390		EMC

Infrastructure teams can see what application they need to recovery in a list that maintains priority score order.

8



ITG Application Infrastructure

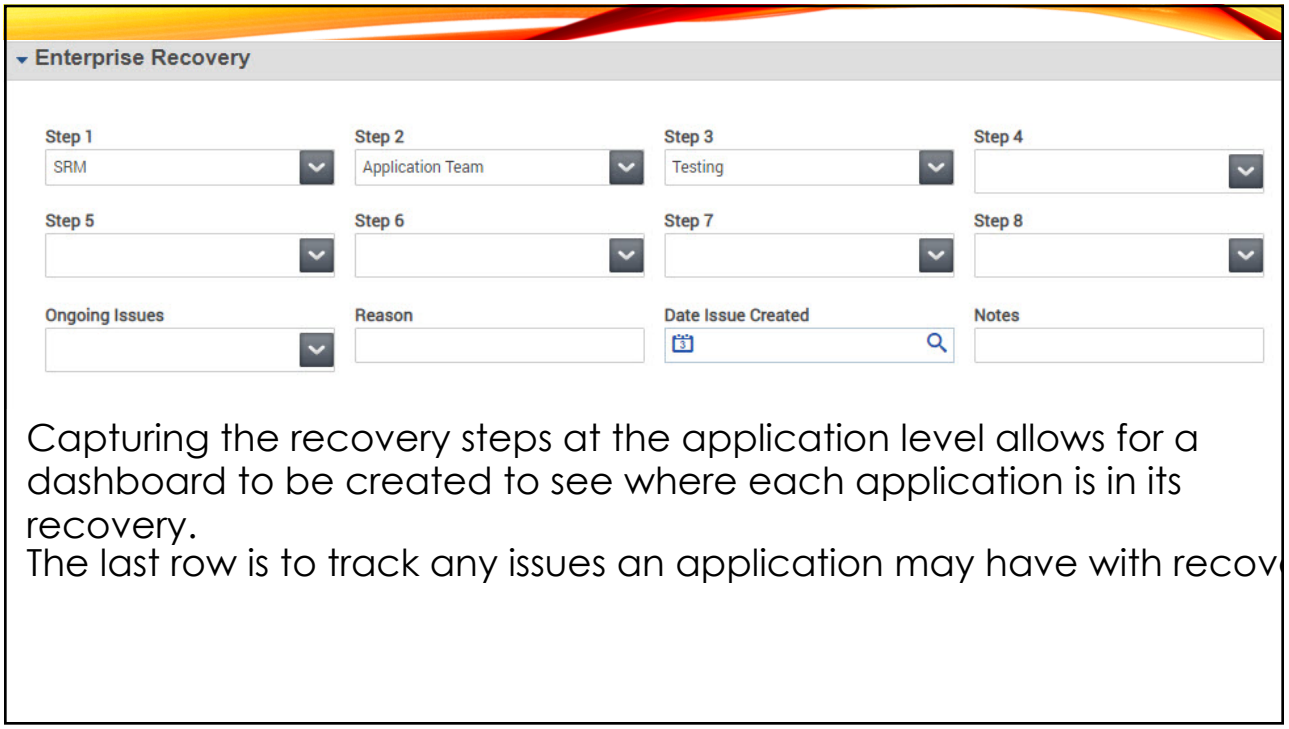
Plan Level Report: This report will show what infrastructure supports every application. 27 Aug 2019

Applications in Plans

PRIORITY SCORE	APPLICATION NAME	STORAGE	WINTEL	AUTOMATION TYPE	UNIX	DBA	MAINFRAME
270		Physical	Physical	N/A	N/A	N/A	N/A
270		N/A	N/A	N/A	N/A	N/A	N/A
250		N/A	Virtual	SRM	N/A	N/A	N/A
250		N/A	Virtual	ZERTO	N/A	N/A	N/A
235		N/A	N/A	N/A	N/A	N/A	N/A
230		Physical	Mixed	ZERTO	Linux	SQL	N/A
230		N/A	Virtual	ZERTO	N/A	SQL	N/A
220		Physical	Mixed	ZERTO	N/A	N/A	N/A

It allows for overall infrastructure needs for all applications to be captured as well.

9

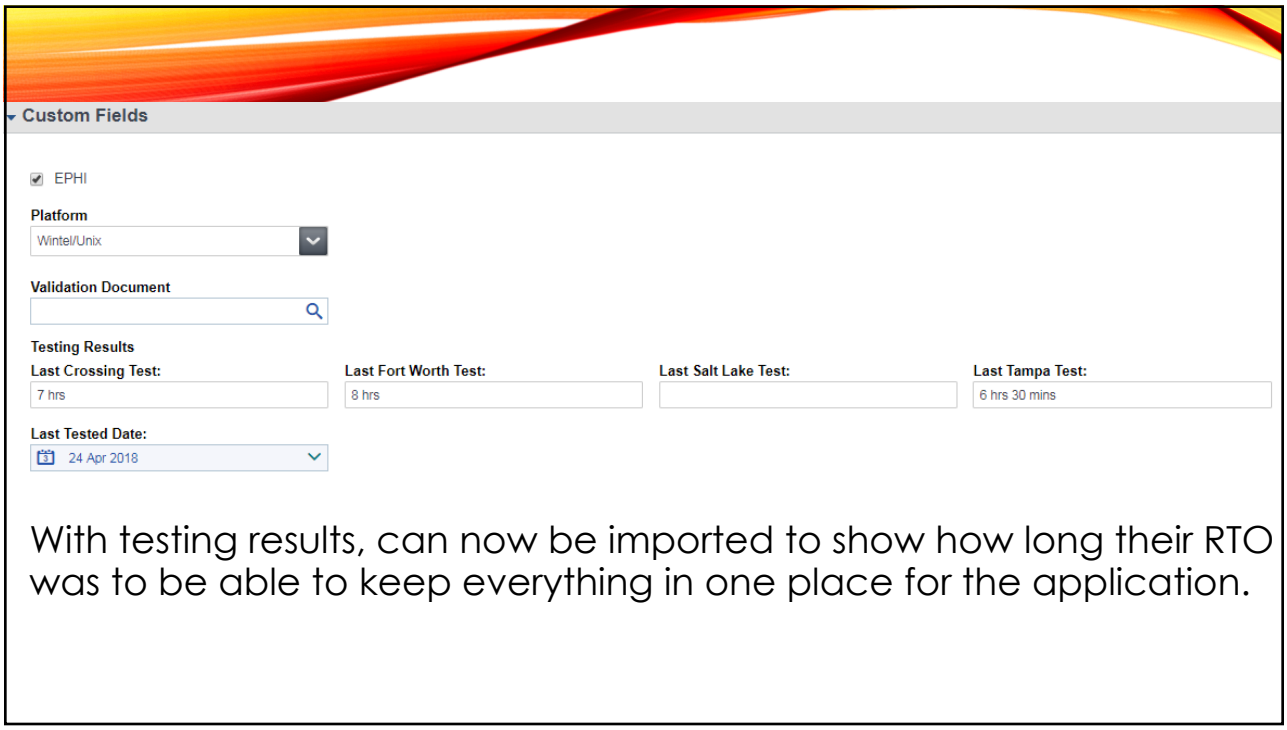


Enterprise Recovery

Step 1	Step 2	Step 3	Step 4
SRM	Application Team	Testing	
Step 5	**Step 6**	**Step 7**	**Step 8**
Ongoing Issues	**Reason**	**Date Issue Created**	**Notes**

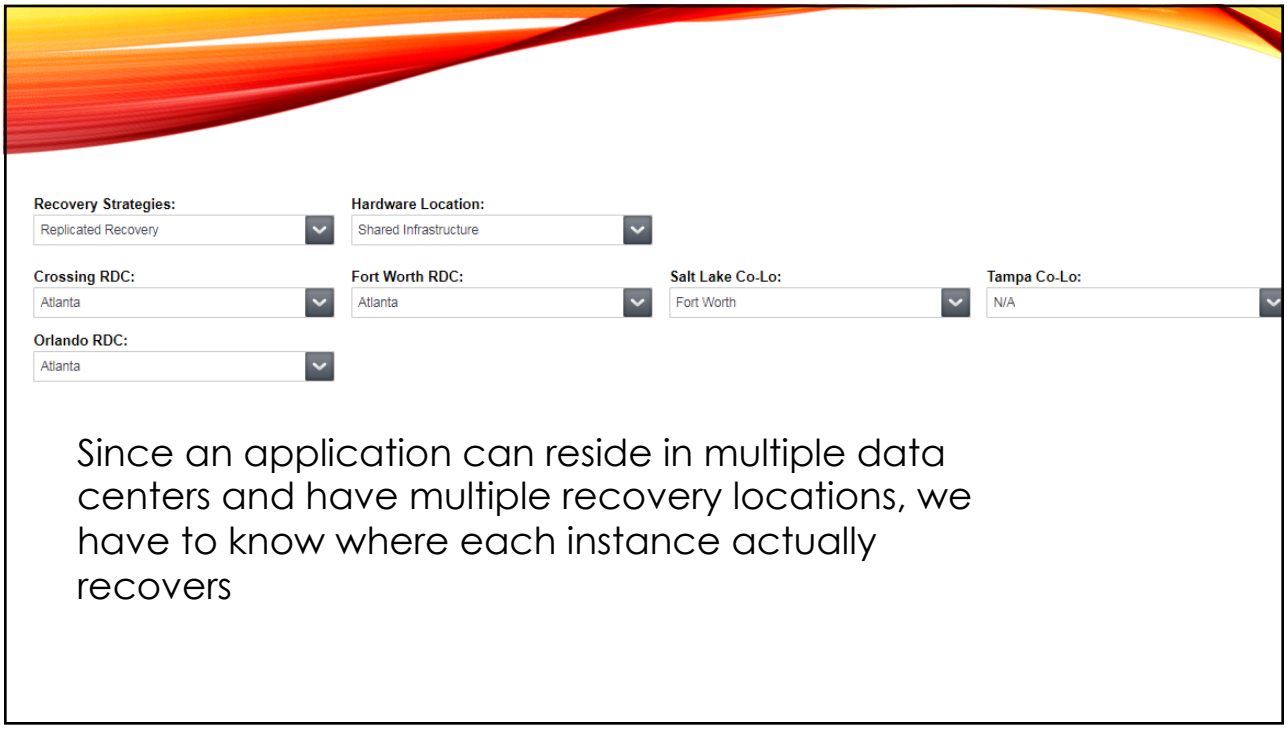
Capturing the recovery steps at the application level allows for a dashboard to be created to see where each application is in its recovery.
The last row is to track any issues an application may have with recov

10



With testing results, can now be imported to show how long their RTO was to be able to keep everything in one place for the application.

11



Since an application can reside in multiple data centers and have multiple recovery locations, we have to know where each instance actually recovers

12

Application to Recovery Location

Plan Level Report: List the Application and What Recovery Location it uses. 27 Aug 2019

PRIORITY SCORE	APPLICATION NAME	ENTERPRISE CRITICALITY	RECOVERY STRATEGIES:	HARDWARE LOCATION:	RDC:
270		01-Mission Critical	Auto Failover	Dedicated Infrastructure	Fort Worth
270		01-Mission Critical	Auto Failover	Dedicated Infrastructure	Fort Worth
250		01-Mission Critical	Replicated Recovery	Dedicated Infrastructure	Atlanta
250		01-Mission Critical	Replicated Recovery	Shared Infrastructure	Atlanta
235		01-Mission Critical	Auto Failover	Dedicated Infrastructure	Fort Worth
230		01-Mission Critical	Replicated Recovery	Shared Infrastructure	Atlanta
230		01-Mission Critical	Replicated Recovery	Dedicated Infrastructure	Atlanta
220		01-Mission Critical	Replicated Recovery	Dedicated Infrastructure	Atlanta

Not having everything recover to the same location out of the data center means that multiple locations may have to be tested when doing a test.

13

PLAN MAINTENANCE

- Now once an application is added to the plan, all the work is done
- The reports do all of the maintenance for me, which allows for my time to be spent working with business owners and application owners education and coordinating testing.
- Audits of the plans are so much easier to review and test against.

14

15

16

6 TO 10 WEEKS OUT

- Select the Location to test
- Determine the objectives for the exercise
- Any possible application should be left on the objectives
- Use this Objectives list to send out with the request for resources

17

Enterprise Application Listing by Priority Score

Plan Level Report: To pull application data by application production location in priority order.

PRIORITY SCORE	APPLICATION NAME	ENTERPRISE CRITICALITY	ACCEPTED RTO	PLATFORM	RECOVERY STRATEGIES :	HARDWARE LOCATION:	AIA LAST UPDATED	APPLICATION ID
270		01-Mission Critical	0 - 8 Hours	Other	Auto Failover	Dedicated Infrastructure	12 Nov 2018	CORPITG0494
270		01-Mission Critical	0 - 8 Hours	Other	Auto Failover	Dedicated Infrastructure	12 Nov 2018	CORPITG0500
250		01-Mission Critical	0 - 8 Hours	Wintel	Replicated Recovery	Dedicated Infrastructure	03 Jul 2018	CORPITG0505
250		01-Mission Critical	0 - 8 Hours	Wintel	Replicated Recovery	Shared Infrastructure	03 Jul 2018	CORPITG0648
235		01-Mission Critical	0 - 8 Hours	Other	Auto Failover	Dedicated Infrastructure	15 Oct 2018	CORPITG0593
230		01-Mission Critical	0 - 8 Hours	Wintel/Unix	Replicated Recovery	Shared Infrastructure	28 Nov 2018	CORPITG0501
230		01-Mission Critical	0 - 8 Hours	Wintel	Replicated Recovery	Dedicated Infrastructure	29 Jun 2018	CORPITG0492
225		01-Mission Critical	0 - 8 Hours	Wintel	Manual Failover	Dedicated Infrastructure	02 Aug 2018	CORPITG0510
220		01-Mission Critical	0 - 8 Hours	Wintel	Replicated Recovery	Dedicated Infrastructure	28 Nov 2018	CORPITG0570
210		01-Mission Critical	0 - 8 Hours	Linux	Replicated Recovery	Shared Infrastructure	21 Jun 2018	CORPITG0612

18

6 TO 10 WEEKS OUT

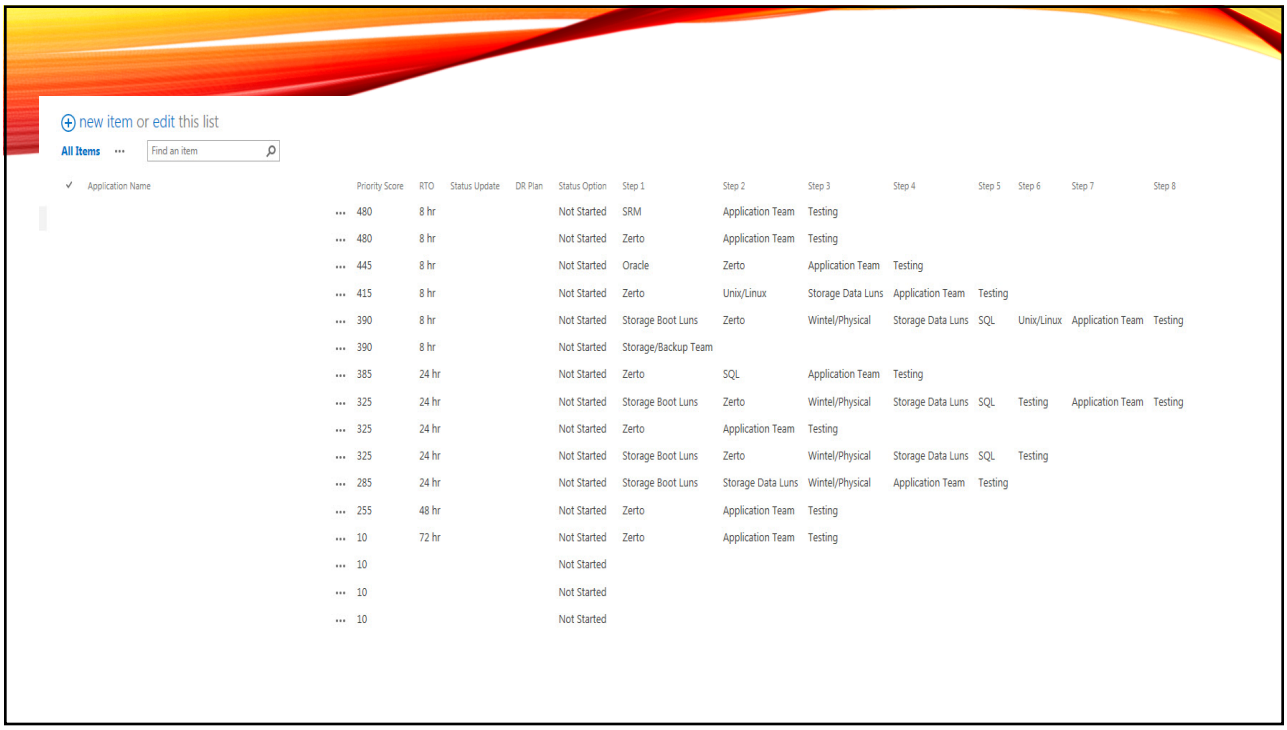
- Create a resource request email and attach the objectives
  - Infrastructure
  - Applications for end user testing
    - Insert Email
  - Boo

19

4 TO 6 WEEKS OUT

- Follow good change management processes
  - Submit any necessary tickets
  - Create all tasks needed
- Develop Tracking Area for the test
  - Add Steps
  - Recovery Procedures
  - Documents

20



new item or edit this list

All Items ··· Find an item

Application Name	Priority Score	RTO	Status Update	DR Plan	Status Option	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
	480	8 hr			Not Started	SRM	Application Team	Testing					
	480	8 hr			Not Started	Zerto	Application Team	Testing					
	445	8 hr			Not Started	Oracle	Zerto	Application Team	Testing				
	415	8 hr			Not Started	Zerto	Unix/Linux	Storage Data Luns	Application Team	Testing			
	390	8 hr			Not Started	Storage Boot Luns	Zerto	Wintel/Physical	Storage Data Luns	SQL	Unix/Linux	Application Team	Testing
	390	8 hr			Not Started	Storage/Backup Team							
	385	24 hr			Not Started	Zerto	SQL	Application Team	Testing				
	325	24 hr			Not Started	Storage Boot Luns	Zerto	Wintel/Physical	Storage Data Luns	SQL	Testing	Application Team	Testing
	325	24 hr			Not Started	Zerto	Application Team	Testing					
	325	24 hr			Not Started	Storage Boot Luns	Zerto	Wintel/Physical	Storage Data Luns	SQL	Testing		
	285	24 hr			Not Started	Storage Boot Luns	Storage Data Luns	Wintel/Physical	Application Team	Testing			
	255	48 hr			Not Started	Zerto	Application Team	Testing					
	10	72 hr			Not Started	Zerto	Application Team	Testing					
	10				Not Started								
	10				Not Started								
	10				Not Started								

21

4 TO 6 WEEKS OUT

- Follow up with Managers about resources
  - You will have to stay on top of them
- Reserve your command center space
- Verify your objectives are still on track
  - If you have to remove an application, make sure that are tracked to a follow up test

22

2 WEEKS OUT

- Send out meeting invites to all assigned resources
- Conduct Tester Training
- Make sure your crisis communication team is involved
- Order meals for resources on site

23

TESTER TRAINING

- Giving testers training before the test helps answer any questions about the DR environment
- Explain to the testers how to access the environment, what can and cannot be tested
- It also allows for explanation of what testing is and why do we do it

24

25

DR ENVIRONMENT SET UP

- Foundation items set up before the clock starts
  - Active Directory
  - Network/DNS
  - Term Servers/Access to DR Environment for Testers
- Command Center Set Up

26

KICKOFF

- Leadership and Test Resources are informed of the following
  - Objectives
  - How Long testing will proceed
  - Timing of Status Updates
  - How information will be communicated
  - Task list handed out to Management/Team Leads
- The Crisis Communication/ Incident Management plan should be used here to make sure everyone is informed

27

STATUS UPDATES

- A conference bridge is engaged will applications are recovering
- Top of the hour updates which are announced on the kickoff call help keep everyone on track
- Any applications in current recovery status get an update
- Once they move to testers, no longer reported on status updates

28

RECOVERY

- Making sure you get the updates on each application can be difficult
- It is helpful to have a scribe in the room to listen for the times of recovery
- Testers most times do not work the same hours as the recovery engineers
- If people take breaks, make sure that is documented for timing purposes

29

TRACKER

Application listing

new item or edit this list

Application Name	Priority Score	RTO	Status Update	DR Plan	Status Option	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
Application A	250	0 - 8 Hours	Complete -		Complete	SRM	Application Team	Testing					
Application B	250	0 - 8 Hours	Complete - 25 minutes		Complete	Zerto - 8:18	Application Team	Testing					
	230	0 - 8 Hours	Will Pick up in the morning		In Progress	Storage Boot Luns - 8:25	Zerto - 8:34	Wintel/Physical	Storage Data Luns	SQL	Unix/Linux	Application Team	Testing
	230	0 - 8 Hours	Complete - 3 hours		Complete	Zerto - 8:43	SQL	Unix/Linux	Application Team				
	230	0 - 8 Hours	- 3 Hours		In Progress	Zerto - 9:00	SQL	Application Team					
	210	0 - 8 Hours	Complete		Complete	Zerto - 8:59	Application Team	Testing					
	210	0 - 8 Hours	Complete - 3 hours		Complete	Zerto - 11:00	Application Team	Testing					
	190	0 - 8 Hours	Complete		Complete	Zerto	Unix/Linux	Storage Data Luns	Application Team	Testing			
	190	0 - 8 Hours	Complete - 7 hours		Complete	Oracle	Zerto - 9:15	Application Team	Testing				
	180	0 - 8 Hours	Ready for restores		Complete								
	170	0 - 8 Hours	Complete -		Complete	Storage Boot Luns - 8:46	Zerto - 9:15	Wintel/Physical	Storage Data Luns	SQL	Testing		
	165	8 - 24 Hours	Ready for Testing		Ready for Testing	Zerto - 11:00	SQL	Application Team-3:39	Testing				
	165	8 - 24 Hours	is working on this morning		Ready for Testing	Storage Boot Luns-8:50	Zerto - 11:17	Wintel/Physical	Storage Data Luns	SQL	Application Team	Testing	

30

ISSUES

- Three types of issues typically seen:
  - Test
  - Recovery
  - Environment
- Need to document all of the issues to determine what needs to go into the report and what needs to be followed up individually

31

AFTER THE TEST

32

FOLLOW UP

- Once the test concludes, it is important to follow up on the following items:
  - Any unresolved issues
  - All Documentation Updates
  - Any Delays in the recovery process that were not documented
- How can you continue to improve the testing?
- Any applications that were removed from the objectives have a follow up test date.

33

TEST REPORT

- To Wrap up the test, a report is created and released to leadership
- The Report Contains:
  - Overview
  - Objectives
  - Test Results
  - Issues
  - Recommendation

34

Application Name	Enterprise Criticality	RTO	Priority Score	Recovery Strategy	Operating System	Recovery Time Achieved	Recovery Successful	Validated Successful	Issues
	Mission Critical	0 - 8 Hours	250	Replicated	Magic	See Below			
						3 hrs	✔	✔	
						9 hrs	✔	✔	
	Mission Critical	0 - 8 Hours	250	Replicated	Wintel	1 hrs	✔	✔	
	Mission Critical	0 - 8 Hours	230	Replicated	Wintel/ Linux	24 hrs	✔	✔	
	Mission Critical	0 - 8 Hours	210	Replicated	Wintel	1 hr	✔	✔	
	Mission Critical	0 - 8 Hours	190	Replicated	Wintel/Unix	5 hrs	✔	✔	
	Mission Critical	0 - 8 Hours	180	Replicated	Wintel	2 hrs	✔	✔	
	Mission Critical	0 - 8 Hours	170	Replicated	Wintel	6 hrs 55 mins	✔	✔	
	Moderate	24 – 48 Hours	58	Replicated	UNIX/AIX /Linux	1 hr	✔	✔	

35

QUESTIONS?

Thank You!!!!

Ray.Holloman@HCAHealthcare.com

36