A Symbol of Excellence

Service Desk Institute
17th September 2020

Disaster Recovery

‘A practical approach’

William Doyle

Head of Disaster Recovery

ICON Plc

ICON Plc

ICON's mission is to help our clients to accelerate the development of drugs and devices that save lives and improve quality of life.

ICON is a global provider of outsourced clinical development and commercialisation services to pharmaceutical, biotechnology, medical device and government and public health organisations.

From a small team of 5 people in 1990, ICON now employs over 15,150 people across 97 locations in 38 countries.

ICON

A Symbol of Excellence

The ICON Disaster Recovery Journey 2018 - Present

1. Why
2. Where to start
3. Interim Plan
4. Core Technologies Review
5. Long Term Plan
6. Play Book
7. Continuous Improvement

Why

- Effects of a disaster
    - Direct damage, inaccessibility, utility outage(power, water, gas etc.)
    - Evacuations, worker absenteeism
    - Loss of revenue

- Regulations/ Standards
    - ISO 27031
    - HIPAA
    - PCI DSS
    - CRF Part 11 Validation
    - Audit
    - RFI & tenders

- Benefits
    - Improved Business processes
    - Improved technologies
    - Fewer service disruptions
    - Better quality of service
    - Competitive advantage
    - Increased business wins

Where to start

Create a Strategy or 'Plan of Action' for Disaster Recovery

- Full review of existing documentation/ processes & procedures

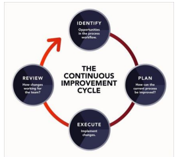
- Full review of Business critical applications

- Clear picture of the Technical capabilities/ commitments & challenges

- Create Interim Plan
  - Implement

- Create Long Term Plan
  - Implement

- Continuous Improvement



THE CONTINUOUS IMPROVEMENT CYCLE

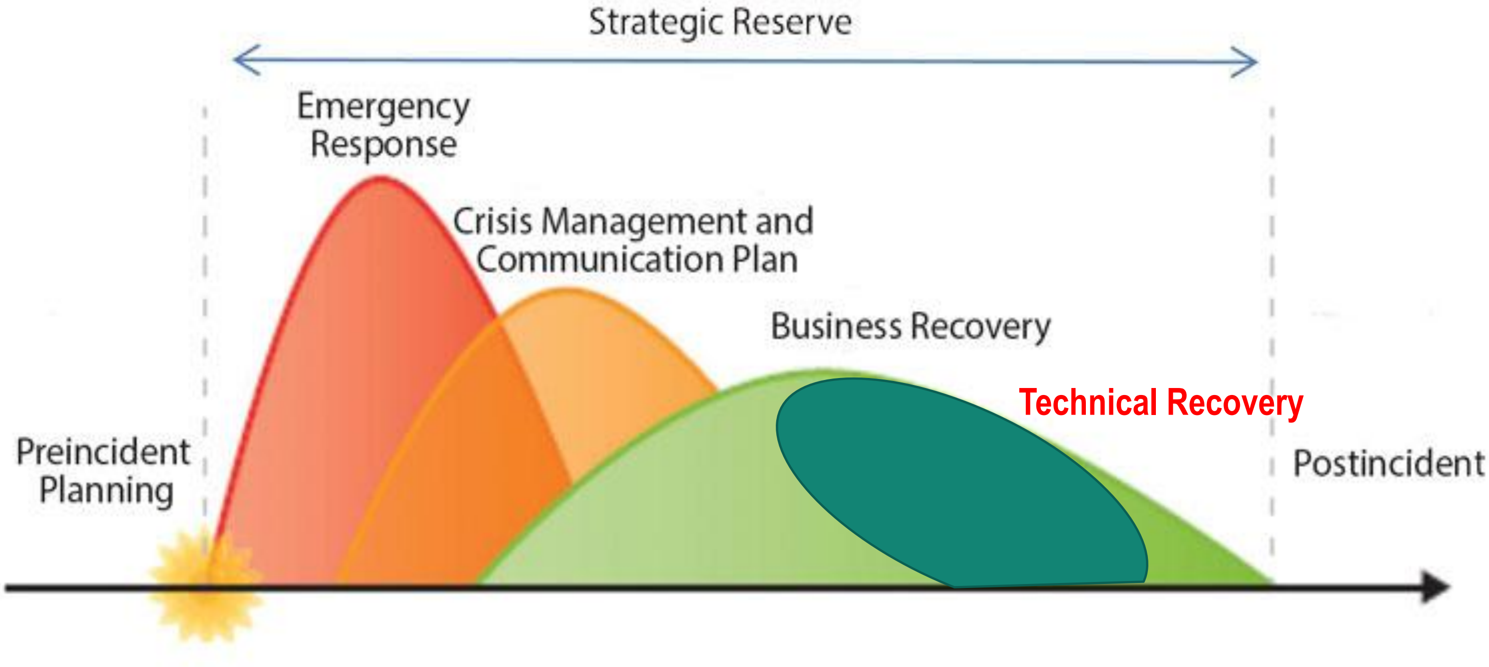
IDENTIFY
Opportunities in the process workflow.

PLAN
How can the current process be improved?

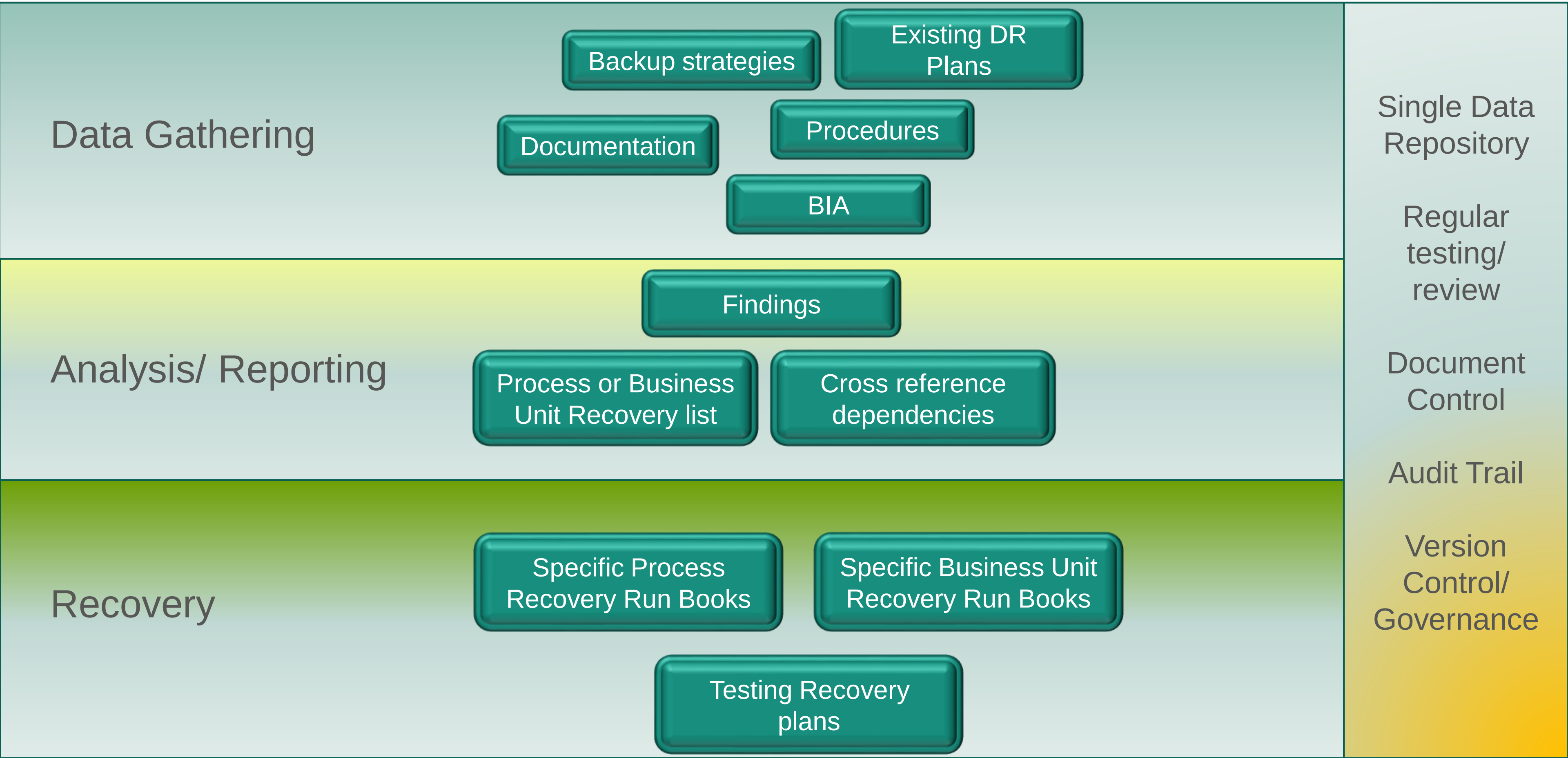
EXECUTE
Implement changes.

REVIEW
How changes working for the team?

Pieces of the Jigsaw



Information Gathering & analysis



Data Gathering

Backup strategies

Existing DR Plans

Documentation

Procedures

BIA

Analysis/ Reporting

Findings

Process or Business Unit Recovery list

Cross reference dependencies

Recovery

Specific Process Recovery Run Books

Specific Business Unit Recovery Run Books

Testing Recovery plans

Single Data Repository

Regular testing/ review

Document Control

Audit Trail

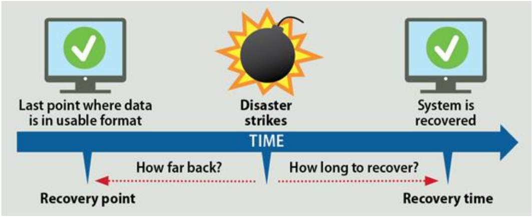
Version Control/ Governance

IT Recovery Capability versus IT Technologies - Review

Recovery Tiers	Recovery Time Objective	Recovery Point Objective	Technical Standards to Meet the Recovery Objective
1	4 Hours	1 Hour	✸ Data Replication At Least Every 1 Hour • Hot Database Standby Available in Alternate Site ✷ Application Switch Over is Automated
2	12 Hours	4 Hours	✸ Data Replication Every 4 Hours • Manual Application Switch Over
3	72 Hours	24 Hours	• Data Replication Every 24 Hours • Recovery From Tape or Disk • Manual Application Switch Over

✸ To be reviewed for Tier 1/2 applications

✷ To confirm if automated or ‘scripts’ are required



Disaster Recovery Interim Plan

1. Align Disaster Recovery Tiers to technical capabilities
2. Baseline Applications to Tier based on Recovery documentation
3. Update entries (System Tier/ RTO/ RPO) in Service Now
4. Update Standard Operating Procedures in EDMS
5. Create/ edit Recovery Run Books for Tier 1 & 2 applications
6. Perform Disaster Recovery tests for all Tier 1 & 2 applications
7. Test all IT Core Backup & Recovery processes (Tier 3 applications)
8. Deliver a Signed “Disaster Recovery Test Certificate” for all completed Recovery tests

Core IT Technologies Review

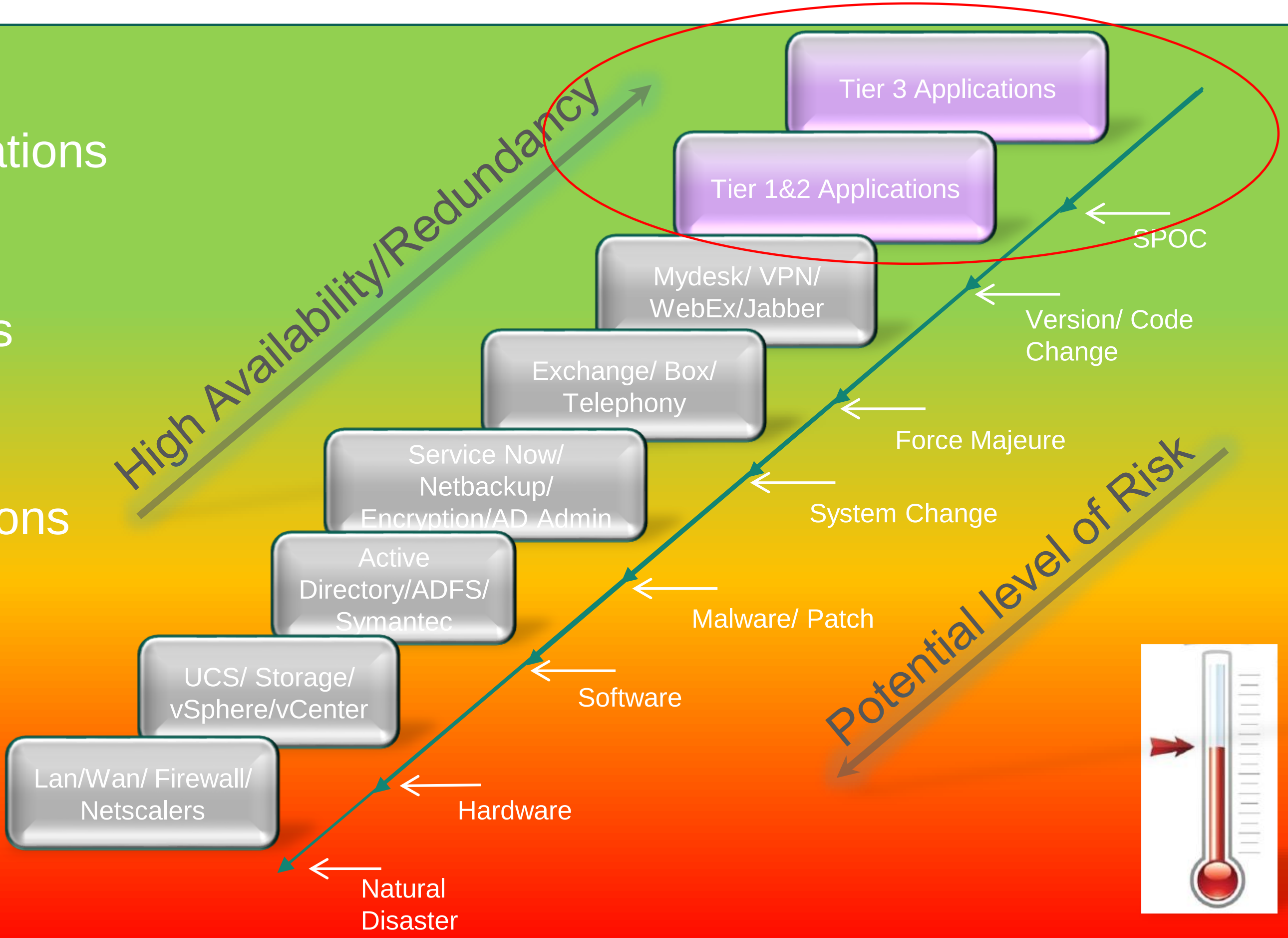
Overall IT Disaster Recovery Risk Register

Core Business Applications

Core User Applications

Core System Applications

Core Infrastructures



High Availability/Redundancy

Tier 3 Applications

Tier 1&2 Applications

Mydesk/ VPN/ WebEx/Jabber

Exchange/ Box/ Telephony

Service Now/ Netbackup/ Encryption/AD Admin

Active Directory/ADFS/ Symantec

UCS/ Storage/ vSphere/vCenter

Lan/Wan/ Firewall/ Netscalers

SPOC

Version/ Code Change

Force Majeure

System Change

Malware/ Patch

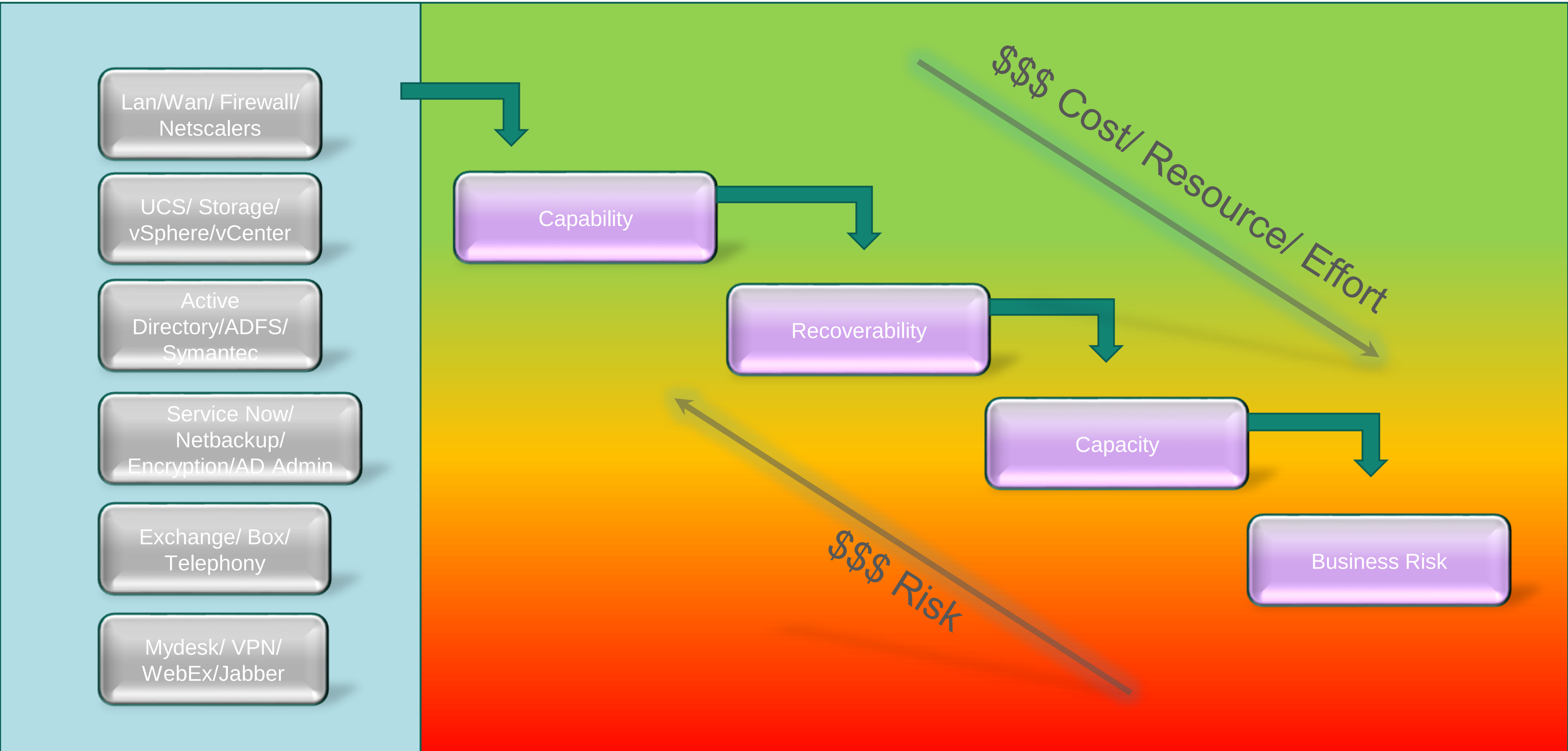
Software

Hardware

Natural Disaster

Potential level of Risk

Full Analysis/ Capability & Risk Register by Technology



Lan/Wan/ Firewall/ Netscalers

UCS/ Storage/ vSphere/vCenter

Active Directory/ADFS/ Symantec

Service Now/ Netbackup/ Encryption/AD Admin

Exchange/ Box/ Telephony

Mydesk/ VPN/ WebEx/Jabber

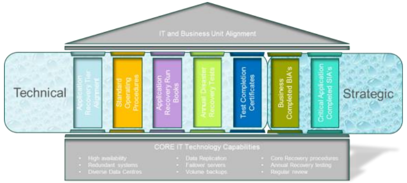
IT Disaster Recovery Core IT Systems & Backup/Restore Tests

Platform	*Name*	*Recovery Order*	*SOP*
CORE DC Infrastructure Lan/Wan/ Firewall/ Netscalers UCS/ Storage/Key Servers vSphere/vCenter Active Directory/ADFS/ Symantec Enterprise	**Backbone Network MPLS**	**1**	IT113-WP039-T01
	Firewall	**1**	IT113-WP039-T02
	Netscalers	**1**	IT113-WP039-T03
	LAN (Nexus)	**1**	IT113-WP039-T06
	UCS Environment	**2**	IT113-WP039-T04
	Storage (Netapps)	**2**	IT113-WP039-T05
	Key Secure Servers	**2**	IT113-WP039-T07
	vSphere ESXi	**3**	IT113-WP039-T08
	ADFS	**3**	IT113-WP039-T09
	vCenter	3	IT113-WP039-T10
	Active Directory/ Domain Controllers	3	IT113-WP039-T11
	DHCP	3	IT113-WP039-T12
	Symantec Enterprise Protection	3	IT113-WP039-T15
IS System Applications Service Now/ Netbackup/ Encryption/AD Admin	Oracle Enterprise Cloud	4	IT113-WP039-T13
	ServiceNow		
	Mimecast		
	ALTIRIS		
	HP Device Manager		
	Symantec Enterprise Encyption		
	AD Administration Tool		
	ICON New User Tool		
	Symantec Enterprise Vault		
	Snapshot		
	Snapmirror		
	Netbackup		
	Backup exec		
Core User Applications Exchange/VPN/ Jabber/ WebEx Mydesk/Box/ Telephony	AnyConnect VPN	5	IT113-WP039-T14
	Cisco Jabber	6	IT113-WP039-T19
	Exchange	6	IT113-WP039-T16-18
	Verizon WebEx		
	Symantec VIP		
	Solarwinds		
	Mydesk		
	BOX		
	Nortel Telephony		
	UCC Telephony		

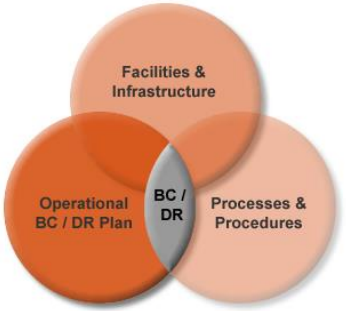
IT Core System Tests	Recovery Procedure
Core Test Circuits	IT113-WP039-T01
Core Test Firewall	IT113-WP039-T02
Core Test Netscaler	IT113-WP039-T03
Core Test UCS	IT113-WP039-T04
Core Test Storage	IT113-WP039-T05
Core Test Lan(Nexus)	IT113-WP039-T06
Core Test Keysecure	IT113-WP039-T07
Core Test vSphere ESXI	IT113-WP039-T08
Core Test ADFS	IT113-WP039-T09
Core Test vCenter	IT113-WP039-T10
Core Test Active Directory	IT113-WP039-T11
Core Test DHCP	IT113-WP039-T12
Core Test Oracle Enterprise Cloud	IT113-WP039-T13
Core Test Anyconnect VPN	IT113-WP039-T14
Core Test Symantec Enterprise Protection	IT113-WP039-T15
Core Test Exchange 2016 (AMDC)	IT113-WP039-T16
Core Test Exchange 2016 (EUDC)	IT113-WP039-T17
Core Test Exchange 2016 (APDC)	IT113-WP039-T18
Core Test Cisco Jabber	IT113-WP039-T19

IT Backup & Restore Tests	Recovery Procedure
Data Archival Process	IT067-WP002
Storage Backup and Restore	IT067-WP005 (v1.0)
Exchange 2016 Backup and Restore	IT067-WP014(1.0)
Oracle Database Backup and Restore	IT067-WP011 (v1.0)
UNIX Physical Backup and Restore	IT067-WP015(1.0)
Windows Physical Backup and Restore	IT067-WP016 (v1.0)
VM Backup and Restore	IT067-WP017 (v1.0)
SQL Database Backup and Restore	IT067-WP018 (v1.0)

Disaster Recovery (Long Term Plan)


IT and Business Unit Alignment
Technical
Application Recovery Tier Alignment
Standard Operating Procedures
Application Recovery Run Books
Annual Disaster Recovery Tests
Test Completion Certificates
Business Completed BIA's
Critical Application Completed SIA's
Strategic
CORE IT Technology Capabilities
High availability
Redundant systems
Diverse Data Centres
Data Replication
Failover servers
Volume backups
Core Recovery procedures
Annual Recovery testing
Regular review

- Create a Structured approach to IT Disaster Recovery (**House of ITDR**)
- Create Recovery Strategy & recovery ‘Run Books’ for all Core IT Technologies (**Core**)
- Implement Application Control Standards for all new or upgraded IT Operations Managed applications (**Process**)
  - IT Position/ Umbrella Statement – Audit/ Acquisition
  - DRP testing completion Certificates
  - Review SaaS/ Vendor Onboarding requirements
  - Schedule annual recovery tests for Tier 1 & 2 Applications and Core IT Technologies
- Support Business Completed BIA’s in Continuity 2 (**Business**)
- Manage a common Single Cloud based ITDR Document Repository for IT Operations (Box etc.)
- Provide structured Disaster Recovery Training/ Certification for IT Staff
- Create a Playbook or Umbrella procedure to support a Disaster Event



IT Operations Activities (Engagement model)

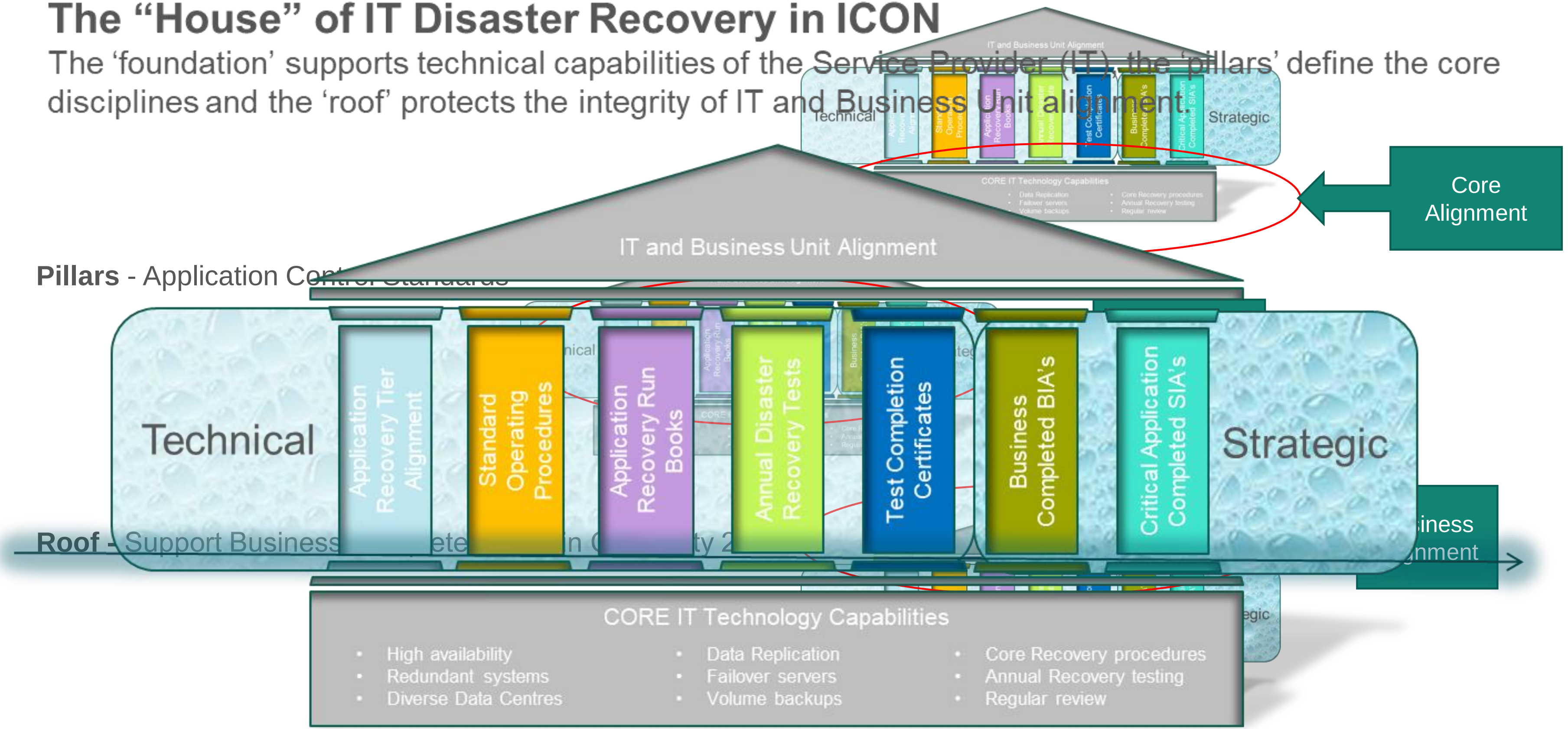
- **Foundation** - Review/ create recovery strategy & *'Run Books'* for all <u>Core IT Technologies</u>

The "House" of IT Disaster Recovery in ICON

The 'foundation' supports technical capabilities of the Service Provider (IT), the 'pillars' define the core disciplines and the 'roof' protects the integrity of IT and Business Unit alignment

- **Pillars** - Application Control Standards

- **Roof** - Support Business



IT and Business Unit Alignment

Technical

Application Recovery Tier Alignment

Standard Operating Procedures

Application Recovery Run Books

Annual Disaster Recovery Tests

Test Completion Certificates

Business Completed BIA's

Critical Application Completed SIA's

Strategic

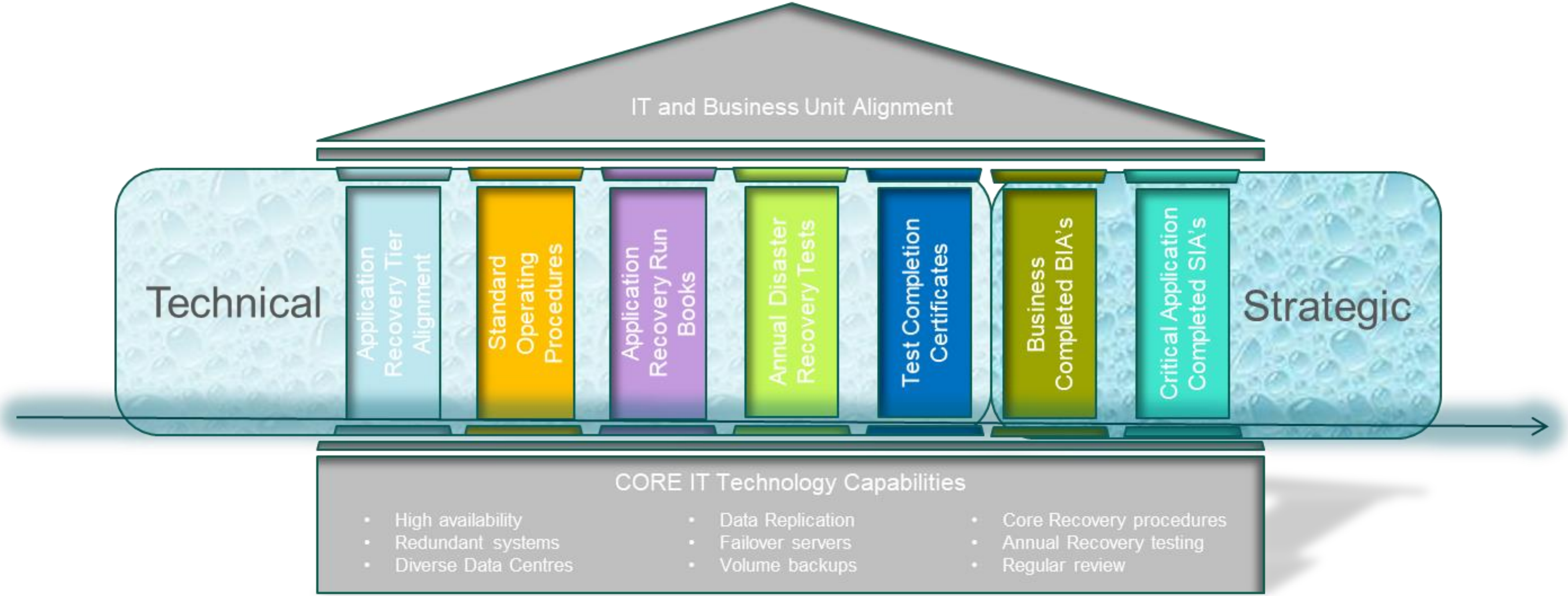
CORE IT Technology Capabilities

- High availability
- Redundant systems
- Diverse Data Centres
- Data Replication
- Failover servers
- Volume backups
- Core Recovery procedures
- Annual Recovery testing
- Regular review

Core Alignment

The “House” of IT Disaster Recovery in ICON

The ‘foundation’ supports technical capabilities of the Service Provider (IT), the ‘pillars’ define the core disciplines and the ‘roof’ protects the integrity of IT and Business Unit alignment.



IT and Business Unit Alignment

Technical

Application Recovery Tier Alignment

Standard Operating Procedures

Application Recovery Run Books

Annual Disaster Recovery Tests

Test Completion Certificates

Business Completed BIA’s

Critical Application Completed SIA’s

Strategic

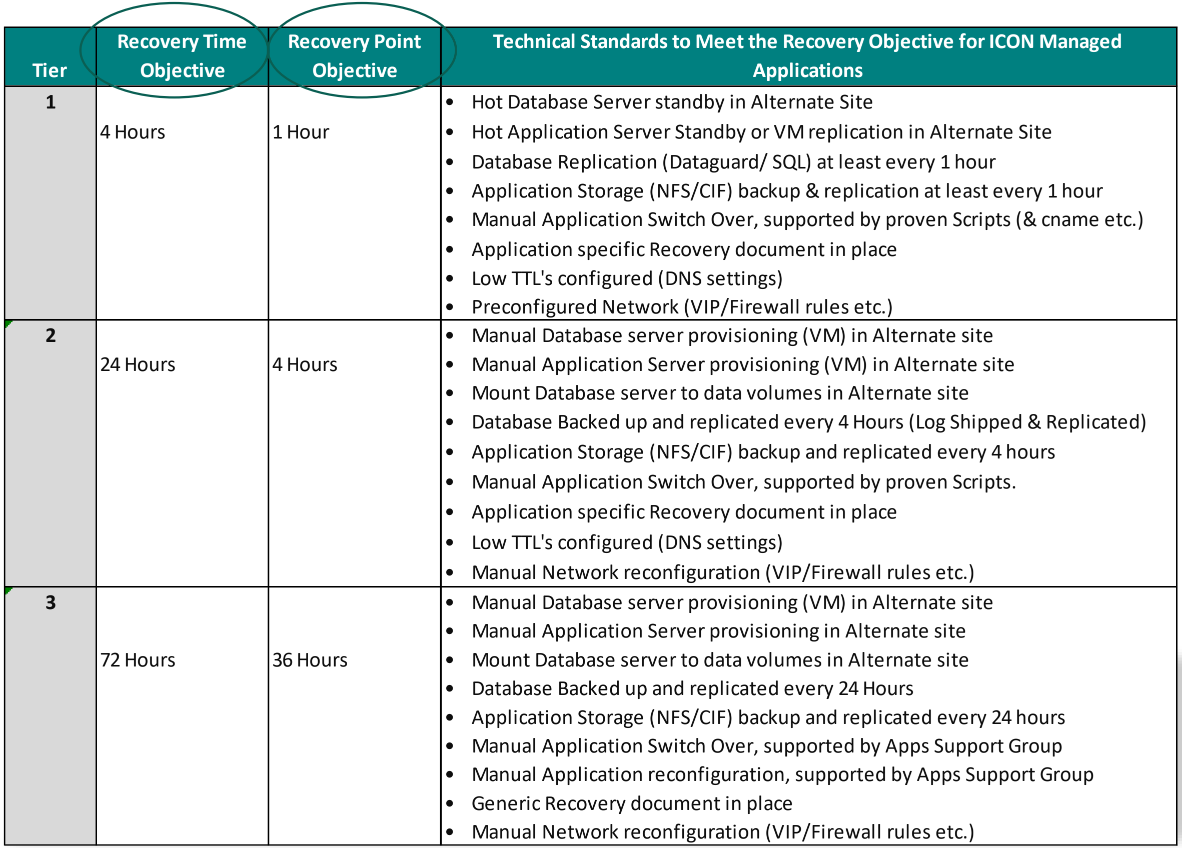
CORE IT Technology Capabilities

- High availability
- Redundant systems
- Diverse Data Centres

- Data Replication
- Failover servers
- Volume backups

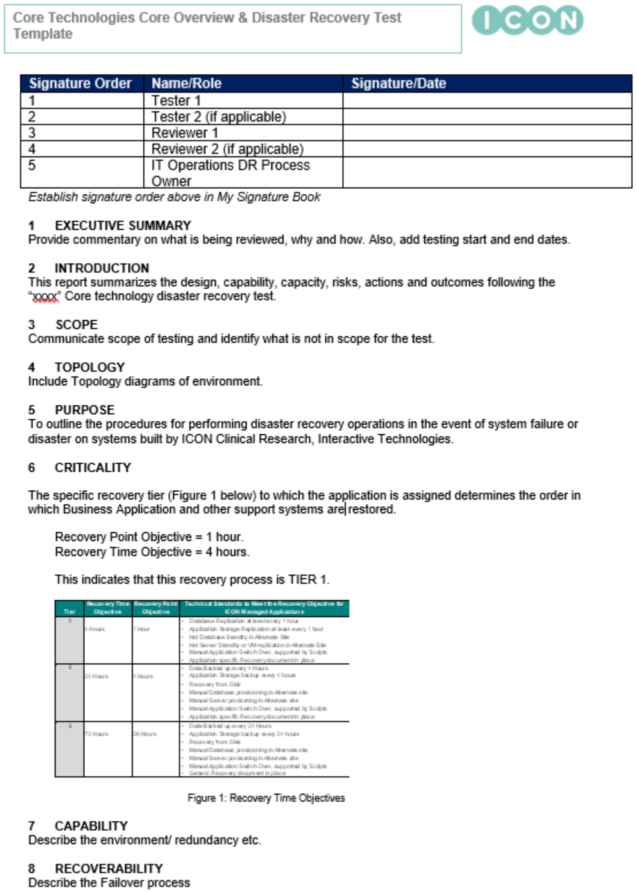
- Core Recovery procedures
- Annual Recovery testing
- Regular review

ICON IT Operations Recovery Tier Table - Final



Tier	Recovery Time Objective	Recovery Point Objective	Technical Standards to Meet the Recovery Objective for ICON Managed Applications
1	4 Hours	1 Hour	• Hot Database Server standby in Alternate Site • Hot Application Server Standby or VM replication in Alternate Site • Database Replication (Dataguard/ SQL) at least every 1 hour • Application Storage (NFS/CIF) backup & replication at least every 1 hour • Manual Application Switch Over, supported by proven Scripts (& cname etc.) • Application specific Recovery document in place • Low TTL's configured (DNS settings) • Preconfigured Network (VIP/Firewall rules etc.)
2	24 Hours	4 Hours	• Manual Database server provisioning (VM) in Alternate site • Manual Application Server provisioning (VM) in Alternate site • Mount Database server to data volumes in Alternate site • Database Backed up and replicated every 4 Hours (Log Shipped & Replicated) • Application Storage (NFS/CIF) backup and replicated every 4 hours • Manual Application Switch Over, supported by proven Scripts. • Application specific Recovery document in place • Low TTL's configured (DNS settings) • Manual Network reconfiguration (VIP/Firewall rules etc.)
3	72 Hours	36 Hours	• Manual Database server provisioning (VM) in Alternate site • Manual Application Server provisioning in Alternate site • Mount Database server to data volumes in Alternate site • Database Backed up and replicated every 24 Hours • Application Storage (NFS/CIF) backup and replicated every 24 hours • Manual Application Switch Over, supported by Apps Support Group • Manual Application reconfiguration, supported by Apps Support Group • Generic Recovery document in place • Manual Network reconfiguration (VIP/Firewall rules etc.)

IT Core Technology Overview/Capability/ Risk & Failover test Plan



Core Technologies Core Overview & Disaster Recovery Test Template

ICON

Signature Order	Name/Role	Signature/Date
1	Tester 1	
2	Tester 2 (if applicable)	
3	Reviewer 1	
4	Reviewer 2 (if applicable)	
5	IT Operations DR Process Owner	

Establish signature order above in My Signature Book

1 EXECUTIVE SUMMARY

Provide commentary on what is being reviewed, why and how. Also, add testing start and end dates.

2 INTRODUCTION

This report summarizes the design, capability, capacity, risks, actions and outcomes following the "xxxx" Core technology disaster recovery test.

3 SCOPE

Communicate scope of testing and identify what is not in scope for the test.

4 TOPOLOGY

Include Topology diagrams of environment.

5 PURPOSE

To outline the procedures for performing disaster recovery operations in the event of system failure or disaster on systems built by ICON Clinical Research, Interactive Technologies.

6 CRITICALITY

The specific recovery tier (Figure 1 below) to which the application is assigned determines the order in which Business Application and other support systems are restored.

Recovery Point Objective = 1 hour.
Recovery Time Objective = 4 hours.

This indicates that this recovery process is TIER 1.

Tier	Recovery Time Objective	Recovery Point Objective	Technical Standards to Meet the Recovery Objective for ICON Managed Applications
1	4 Hours	1 Hour	- Database Replication at least every 1 hour - Application Storage Replication at least every 1 hour - Hot Database Standby in Alternate Site - Hot Server Standby or VM replication in Alternate Site - Manual Application Switch Over, supported by Scripts - Application specific Recovery document in place
2	24 Hours	4 Hours	- Data Backed up every 4 Hours - Application Storage backup every 4 hours - Recovery from Disk - Manual Database provisioning in Alternate site - Manual Server povisioning in Alternate site - Manual Application Switch Over, supported by Scripts - Application specific Recovery document in place
3	72 Hours	36 Hours	- Data Backed up every 24 Hours - Application Storage backup every 24 hours - Recovery from Disk - Manual Database provisioning in Alternate site - Manual Server povisioning in Alternate site - Manual Application Switch Over, supported by Scripts - Generic Recovery document in place

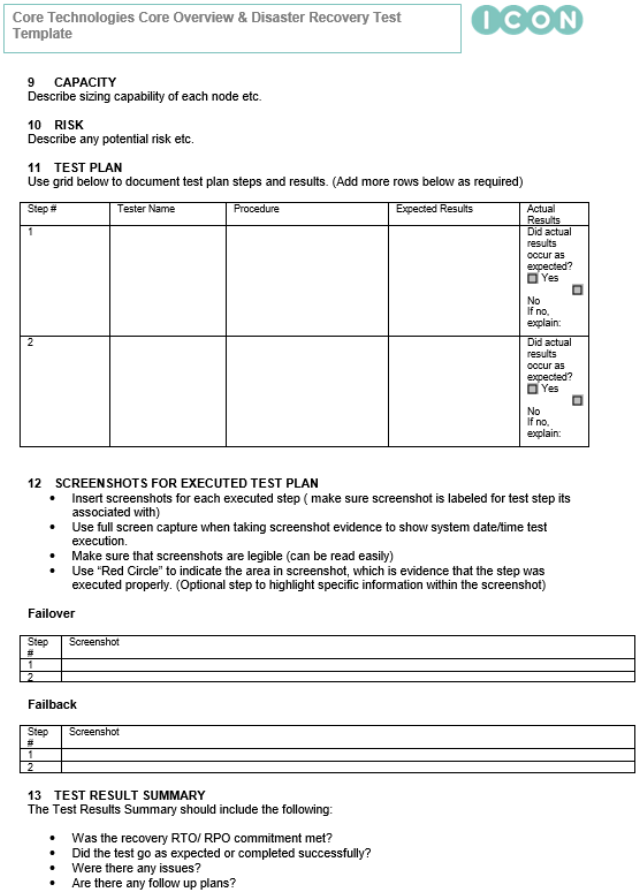
Figure 1: Recovery Time Objectives

7 CAPABILITY

Describe the environment/ redundancy etc.

8 RECOVERABILITY

Describe the Failover process



Core Technologies Core Overview & Disaster Recovery Test Template

ICON

9 CAPACITY

Describe sizing capability of each node etc.

10 RISK

Describe any potential risk etc.

11 TEST PLAN

Use grid below to document test plan steps and results. (Add more rows below as required)

Step #	Tester Name	Procedure	Expected Results	Actual Results
1				Did actual results occur as expected? □ Yes □ No If no, explain:
2				Did actual results occur as expected? □ Yes □ No If no, explain:

12 SCREENSHOTS FOR EXECUTED TEST PLAN

- Insert screenshots for each executed step (make sure screenshot is labeled for test step its associated with)
- Use full screen capture when taking screenshot evidence to show system date/time test execution.
- Make sure that screenshots are legible (can be read easily)
- Use "Red Circle" to indicate the area in screenshot, which is evidence that the step was executed properly. (Optional step to highlight specific information within the screenshot)

Failover

Step #	Screenshot
1	
2	

Failback

Step #	Screenshot
1	
2	

13 TEST RESULT SUMMARY

The Test Results Summary should include the following:

- Was the recovery RTO/ RPO commitment met?
- Did the test go as expected or completed successfully?
- Were there any issues?
- Are there any follow up plans?

IT Operations Application Control Standards

1. Align Application to IT Recovery Tier (RTO/RPO)

2. Update entries (System Tier/ RTO/ RPO) in Service Now

3. Create Standard Operating Procedure for all new applications supported by ICON IT (MetricStream)

4. Review/ Update/ Create Standard Operating Procedures for upgraded Applications, supported by ICON IT

5. Manage an Application Recovery “run-book” for all Tier 1 & 2 or Core IT Applications:

    A. Review/ update existing “run-books” for Tier 1 & 2 Applications, supported by ICON IT

    B. Design & cost system upgrade from a Tier 3 to Tier 1 & 2 level Application

    C. Create “run-books” for upgraded Tier 1 & 2 Applications, supported by ICON IT

    D. Plan Disaster Recovery test for all new Tier 1 & 2 Applications as part of the implementation phase

6. Perform an Annual Disaster Recovery test for all:

    A. Tier 1 & 2 Applications

    B. IT Core platforms (covering Tier 3 Applications)

7. Deliver a Signed “Disaster Recovery Test Certificate” for all completed Recovery tests

IT Disaster Recovery Position Statement – Testing commitments

ICON Disaster Recovery SOP’s

−	IT113-SOP	– IT Disaster Recovery Plan
−	IT113-WP039	– Core Technology Systems Testing
−	IT067-SOP	– Data Backup & Recovery

ICON IT Operations Disaster Recovery Testing Commitments

Disaster Recovery Testing is prioritized within the annual IT Operations project schedule.

ICON will perform annual Disaster Recovery tests for a suite of **Tier 1** and **Tier 2** IT systems, managed by ICON IT Operations.

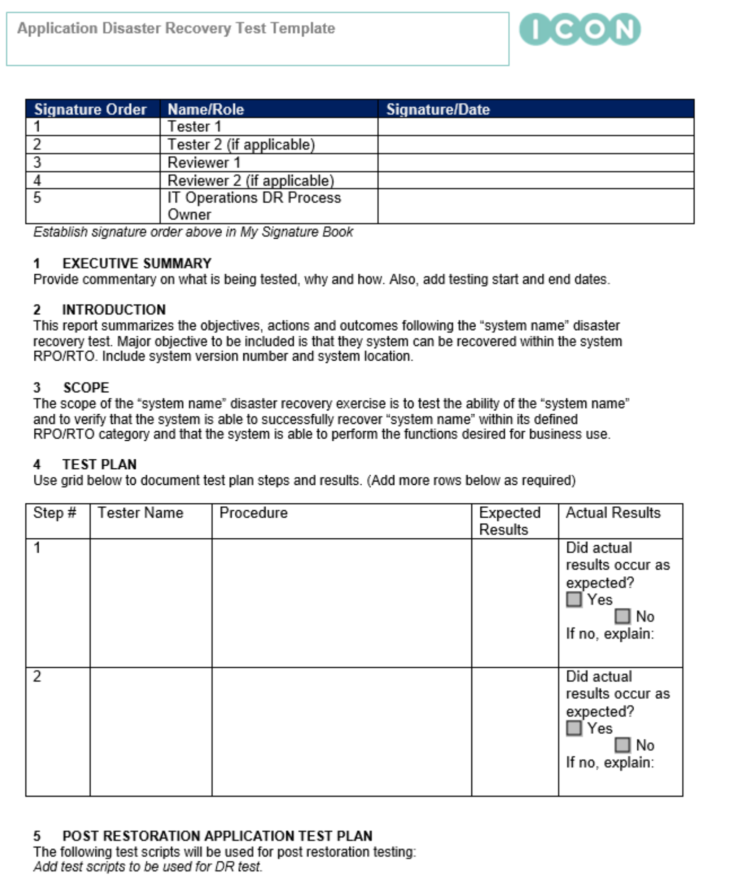
ICON will perform annual Disaster Recovery tests for all **IT Core Technology** and **Technology Specific** systems.

All completed Disaster Recovery tests will have signed completion Test Certificates.

The IT Disaster Recovery Plan (IT113-SOP) and all associated Procedures are controlled documents and managed through ICON’s Electronic Document Management System (Metricstream EDMS).

All ICON Disaster Recovery Testing evidence, project files & Test Certificates are managed and can be found in **Box** under “ICON IT Disaster Recovery”.

Recovery Run Book & schedule DR Test for all Tier 1 & 2 Apps



Application Disaster Recovery Test Template

Signature Order	Name/Role	Signature/Date
1	Tester 1	
2	Tester 2 (if applicable)	
3	Reviewer 1	
4	Reviewer 2 (if applicable)	
5	IT Operations DR Process Owner	

Establish signature order above in My Signature Book

1 EXECUTIVE SUMMARY

Provide commentary on what is being tested, why and how. Also, add testing start and end dates.

2 INTRODUCTION

This report summarizes the objectives, actions and outcomes following the "system name" disaster recovery test. Major objective to be included is that they system can be recovered within the system RPO/RTO. Include system version number and system location.

3 SCOPE

The scope of the "system name" disaster recovery exercise is to test the ability of the "system name" and to verify that the system is able to successfully recover "system name" within its defined RPO/RTO category and that the system is able to perform the functions desired for business use.

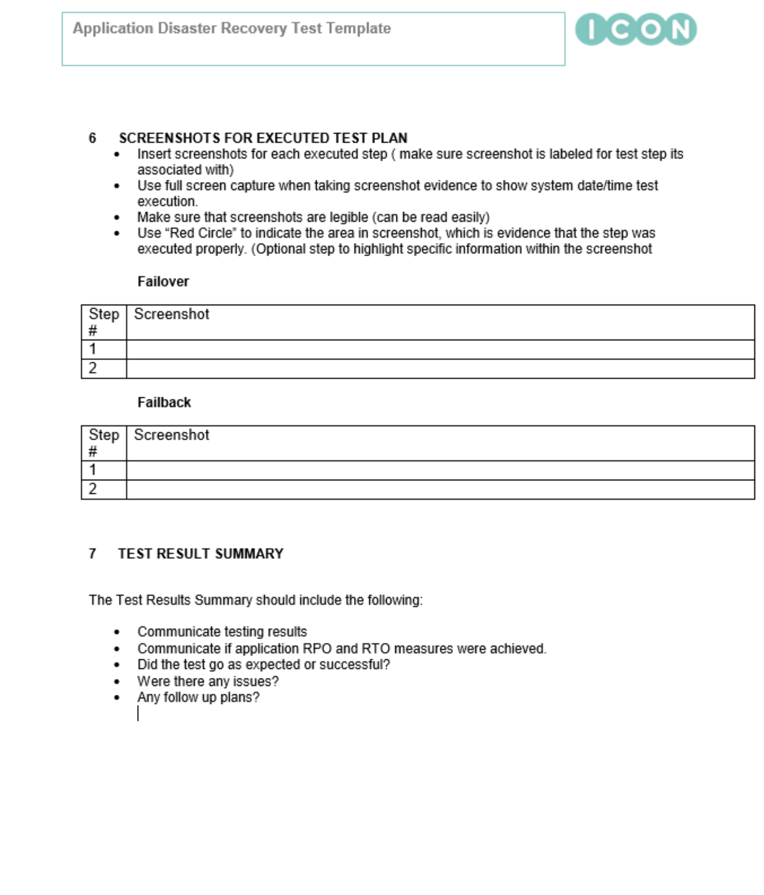
4 TEST PLAN

Use grid below to document test plan steps and results. (Add more rows below as required)

Step #	Tester Name	Procedure	Expected Results	Actual Results
1				Did actual results occur as expected? □ Yes □ No If no, explain:
2				Did actual results occur as expected? □ Yes □ No If no, explain:

5 POST RESTORATION APPLICATION TEST PLAN

The following test scripts will be used for post restoration testing:
Add test scripts to be used for DR test.



Application Disaster Recovery Test Template

6 SCREENSHOTS FOR EXECUTED TEST PLAN

- Insert screenshots for each executed step (make sure screenshot is labeled for test step its associated with)
- Use full screen capture when taking screenshot evidence to show system date/time test execution.
- Make sure that screenshots are legible (can be read easily)
- Use "Red Circle" to indicate the area in screenshot, which is evidence that the step was executed properly. (Optional step to highlight specific information within the screenshot

Failover

Step #	Screenshot
1	
2	

Failback

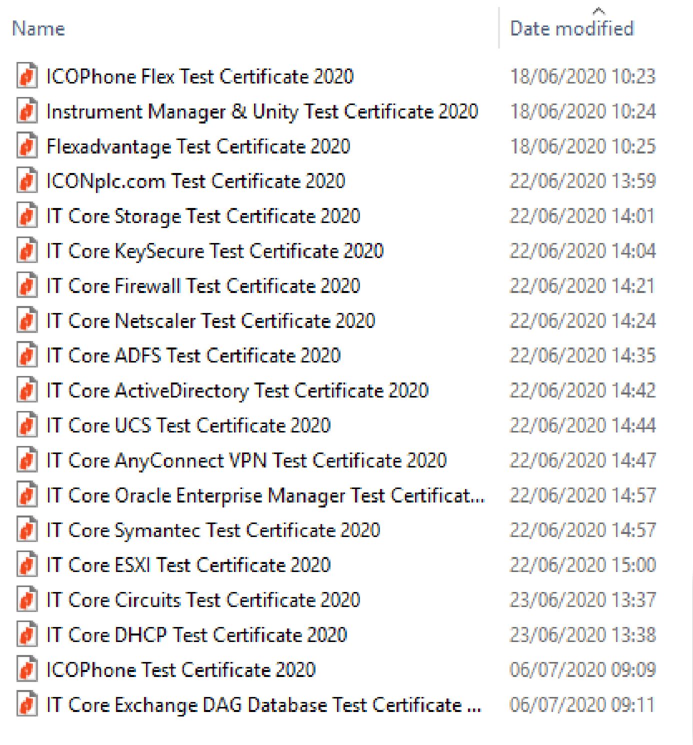
Step #	Screenshot
1	
2	

7 TEST RESULT SUMMARY

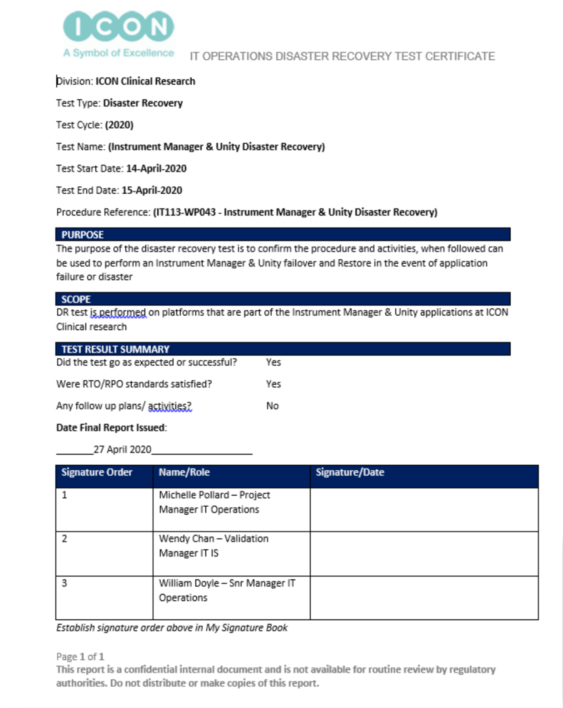
The Test Results Summary should include the following:

- Communicate testing results
- Communicate if application RPO and RTO measures were achieved.
- Did the test go as expected or successful?
- Were there any issues?
- Any follow up plans?

Compliance - IT Disaster Recovery Test Certification



Name	Date modified
ICOPhone Flex Test Certificate 2020	18/06/2020 10:23
Instrument Manager & Unity Test Certificate 2020	18/06/2020 10:24
Flexadvantage Test Certificate 2020	18/06/2020 10:25
ICONplc.com Test Certificate 2020	22/06/2020 13:59
IT Core Storage Test Certificate 2020	22/06/2020 14:01
IT Core KeySecure Test Certificate 2020	22/06/2020 14:04
IT Core Firewall Test Certificate 2020	22/06/2020 14:21
IT Core Netscaler Test Certificate 2020	22/06/2020 14:24
IT Core ADFS Test Certificate 2020	22/06/2020 14:35
IT Core ActiveDirectory Test Certificate 2020	22/06/2020 14:42
IT Core UCS Test Certificate 2020	22/06/2020 14:44
IT Core AnyConnect VPN Test Certificate 2020	22/06/2020 14:47
IT Core Oracle Enterprise Manager Test Certificat...	22/06/2020 14:57
IT Core Symantec Test Certificate 2020	22/06/2020 14:57
IT Core ESXI Test Certificate 2020	22/06/2020 15:00
IT Core Circuits Test Certificate 2020	23/06/2020 13:37
IT Core DHCP Test Certificate 2020	23/06/2020 13:38
ICOPhone Test Certificate 2020	06/07/2020 09:09
IT Core Exchange DAG Database Test Certificate ...	06/07/2020 09:11



ICON
A Symbol of Excellence

IT OPERATIONS DISASTER RECOVERY TEST CERTIFICATE

Division: **ICON Clinical Research**

Test Type: **Disaster Recovery**

Test Cycle: **(2020)**

Test Name: **(Instrument Manager & Unity Disaster Recovery)**

Test Start Date: **14-April-2020**

Test End Date: **15-April-2020**

Procedure Reference: **(IT113-WP043 - Instrument Manager & Unity Disaster Recovery)**

PURPOSE

The purpose of the disaster recovery test is to confirm the procedure and activities, when followed can be used to perform an Instrument Manager & Unity failover and Restore in the event of application failure or disaster

SCOPE

DR test is performed on platforms that are part of the Instrument Manager & Unity applications at ICON Clinical research

TEST RESULT SUMMARY

Did the test go as expected or successful?	Yes
Were RTO/RPO standards satisfied?	Yes
Any follow up plans/ activities?	No

Date Final Report Issued:

________27 April 2020____________________

Signature Order	Name/Role	Signature/Date
1	Michelle Pollard – Project Manager IT Operations	
2	Wendy Chan – Validation Manager IT IS	
3	William Doyle – Snr Manager IT Operations	

Establish signature order above in My Signature Book

Page **1** of **1**

This report is a confidential internal document and is not available for routine review by regulatory authorities. Do not distribute or make copies of this report.

IT and IT Alignment, including Business Stakeholders

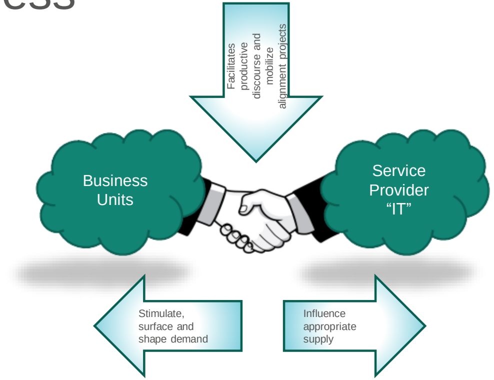
Collaboration– 'to work with another person or group in order to achieve or do something'.

- Virtual teams consisting of multiple disciplines (DBA/ Server/ Storage/ Network, stakeholders, Business testers)
- Cultural nuances
- Shared vision – buy in
- DR Failover test planning, execution & review
- Teamwork – meetings/ workshops
- Communication
- Motivation
- Share success
- Cycle team membership & roles

Business and IT Alignment

Continuity 2 – A Cloud based product managing ICON Business Resumption plans**.**

- Business unit owner completed Business Impact Analysis forms
- IT completed 'System Impact Analysis' for Business highlighted Critical applications
- Application re-aligned to IT Recovery Tier (RTO/RPO)
- Review/ upgrade Application hardware/ software capabilities in-line with new requirements
- Develop an Application Recovery "run-book" for all newly defined Tier 1 & 2 applications
- Perform an Annual Disaster Recovery test for all Tier 1 & 2 applications
- Deliver a Signed "Disaster Recovery Test Certificate" for all completed annual Recovery tests

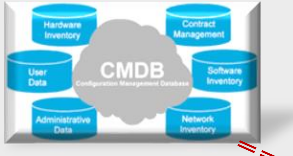

Facilitates productive discourse and mobilize alignment projects
Business Units
Service Provider "IT"
Stimulate, surface and shape demand
Influence appropriate supply

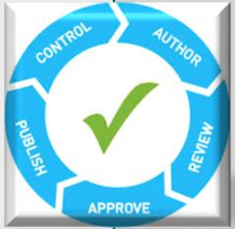
Overall IT Disaster Recovery Architecture Strategy for Business

IT Technical

Inventory

- CI's
- Applications
- Owners
- Business Units





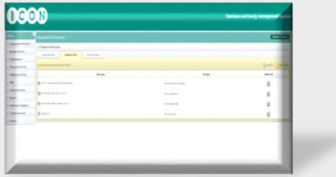
Business/IT completed SIA
(Tier 1 & 2)

Key Product / Service SIA Report for
ICR 90 Clinical - Operations

Critical Process alignment

Associated Recovery Documents

- IT Core Backup & Restore
- Specific Run Books
- Tier 1 & 2 Annual testing & review



Business

Inventory

- Staff
- Contact details
- Service Lines

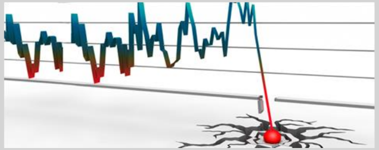
Business completed BIA

Business Impact Analysis Report
C2 Template Testing James

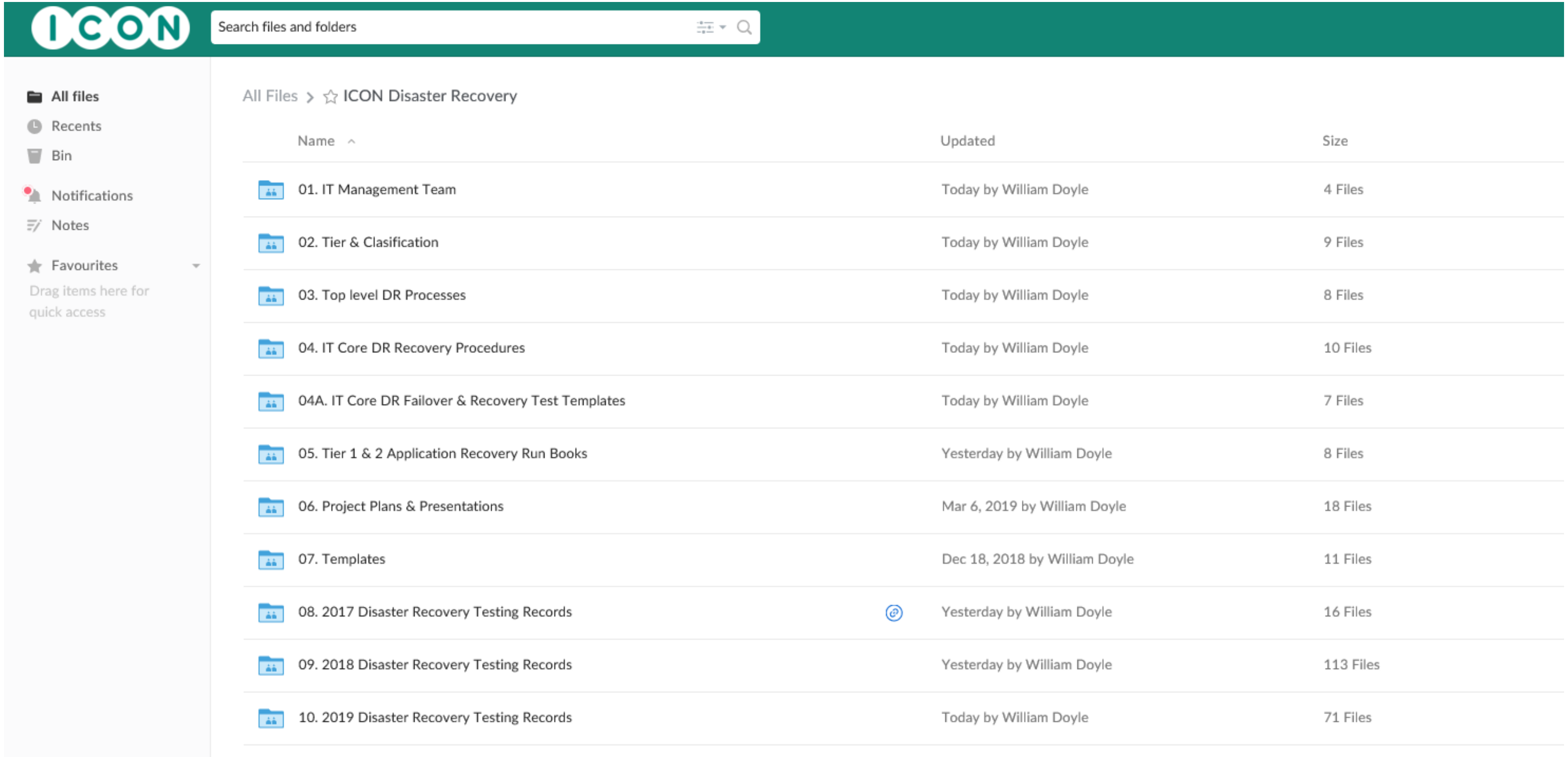
Recovery Tier alignment

Business & IT alignment

"Disaster Recovery planning is not about the technology, it is about the Business"



Single Cloud based ITDR Document Repository for IT Operations



All Files > ☆ ICON Disaster Recovery

Name	Updated	Size
01. IT Management Team	Today by William Doyle	4 Files
02. Tier & Clasification	Today by William Doyle	9 Files
03. Top level DR Processes	Today by William Doyle	8 Files
04. IT Core DR Recovery Procedures	Today by William Doyle	10 Files
04A. IT Core DR Failover & Recovery Test Templates	Today by William Doyle	7 Files
05. Tier 1 & 2 Application Recovery Run Books	Yesterday by William Doyle	8 Files
06. Project Plans & Presentations	Mar 6, 2019 by William Doyle	18 Files
07. Templates	Dec 18, 2018 by William Doyle	11 Files
08. 2017 Disaster Recovery Testing Records	Yesterday by William Doyle	16 Files
09. 2018 Disaster Recovery Testing Records	Yesterday by William Doyle	113 Files
10. 2019 Disaster Recovery Testing Records	Today by William Doyle	71 Files

IT Operations – Disaster Recovery Achievements 2019

IT Strategic Transformation Initiatives 2019

Focus	Activity	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Notes
Standards	Implement ICON Application Control Standards	■	■	■	■	■	■	■	■	■	■	■	■	Structured Application Portfolio management
	Common single cloud based Document repository	■	■	■	■	■	■	■	■	■	■	■	■	BOX Folders
	IT Disaster Recovery Position Summary									■	■	■	■	Business alignment
Operational	Review Vendor Onboarding process	■	■	■	■	■	■	■	■	■	■	■	■	Vendor MSA Uptime Commitment / Acceptance
	Review ICON Disaster Recovery Tier & Capabilities	■	■	■	■	■	■	■	■	■	■	■	■	Confirm IT Operations Technical capabilities/abilities
	Annual SaaS Services review					■	■	■	■	■	■	■	■	Vendor Service uptime Risk/ Acceptance
Support	Create Risk & Test templates for all IT Core technologies					■	■	■	■	■	■	■	■	Manage IT Operations Core system capabilities
	Support Protect Initiative							■	■	■	■	■	■	Deliver against IT actions for a Disaster Scenario
	Annual ICON Tier 1 & 2 Disaster Recovery testing		■	■	■	■	■	■	■	■	■	■	■	Perform complete Application failover tests
Strategy	Align IT Ops/ Technology, Process & Business	■	■	■	■	■	■	■	■	■	■	■	■	House of Disaster Recovery model, Ops alignment
	Align Application support expectations with Business						■	■	■	■	■	■	■	Engage Business units i.e. Labs/ Firecrest/ Marketing
	Invest in technology to better support business needs												■	Align IT with Business/ Revenue growth (2019-2020)

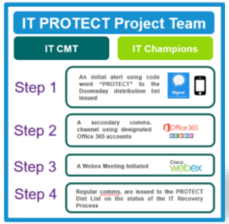
IT Operations Application Control Standards

1. Align Application to IT Recovery Tier (RTO/RPO)
2. Update entries (System Tier/ RTO/ RPO) in Service Now
3. Create Standard Operating Procedure for all new applications supported by ICON IT (MetricStream)
4. Review/ Update/ Create Standard Operating Procedures for upgraded Applications, supported by ICON IT
5. Manage an Application Recovery "run-book" for all Tier 1 & 2 or Core IT Applications:
   A. Review/ update existing "run-books" for Tier 1 & 2 Applications, supported by ICON IT
   B. Design & cost system upgrade from a Tier 3 to Tier 1 & 2 level Application
   C. Create "run-books" for upgraded Tier 1 & 2 Applications, supported by ICON IT
   D. Plan Disaster Recovery test for all new Tier 1 & 2 Applications as part of the implementation phase
6. Perform an Annual Disaster Recovery test for all:
   A. Tier 1 & 2 Applications
   B. IT Core platforms (covering Tier 3 Applications)
7. Deliver a Signed "Disaster Recovery Test Certificate" for all completed Recovery tests

Success to date:

FCS v6
Spotfire
Sailpoint
IRIS
Rees
SAS Grid

Tier	Recovery Time Objective	Recovery Point Objective	Technical Standards to Meet the Recovery Objective for ICON Managed Applications
1	4 Hours	1 Hour	• Database Replication at least every 1 hour • Application Storage Replication at least every 1 hour • Hot Database Standby in Alternate Site • Hot Server Standby or VM replication in Alternate Site • Manual Application Switch Over, supported by Scripts • Application specific Recovery document in place
2	24 Hours	4 Hours	• Data Backed up every 4 Hours • Application Storage backup every 4 hours • Recovery from Disk • Manual Database provisioning in Alternate site • Manual Server provisioning in Alternate site • Manual Application Switch Over, supported by Scripts • Application specific Recovery document in place
3	72 Hours	36 Hours	• Data Backed up every 24 Hours • Application Storage backup every 24 hours • Recovery from Disk • Manual Database provisioning in Alternate site • Manual Server provisioning in Alternate site • Manual Application Switch Over, supported by Scripts • Generic Recovery document in place



IT PROTECT Project Team

IT CMT | IT Champions

Step 1 – An initial alert using code word "PROTECT" to the Doomsday distribution list issued

Step 2 – A secondary comms. channel using designated Office 365 accounts

Step 3 – A Webex Meeting Initiated

Step 4 – Regular comms. are issued to the PROTECT Dist List on the status of the IT Recovery Process

Platform	*Name*	*Recovery Order*	*SOP*
CORE DC Infrastructure Lan/Wan/ Firewall/ Netscalers UCS/ Storage/Key Servers vSphere/vCenter Active Directory/ADFS/ Symantec VIP	**Backbone Network MPLS**	**1**	IT113-WP039-T01
	Firewall	**1**	IT113-WP039-T02
	Netscalers	**1**	IT113-WP039-T03
	LAN (Nexus)	**1**	IT113-WP039-T06
	UCS Environment	**2**	IT113-WP039-T04
	Storage (Netapps)	**2**	IT113-WP039-T05
	Key Secure Servers	**2**	IT113-WP039-T07
	vSphere ESXi	**3**	IT113-WP039-T08
	ADFS	**3**	IT113-WP039-T09
	vCenter	3	IT113-WP039-T10
	Active Directory/ Domain Controllers	3	
	DHCP	3	

IT Operations Disaster Recovery Position Summary

ICON

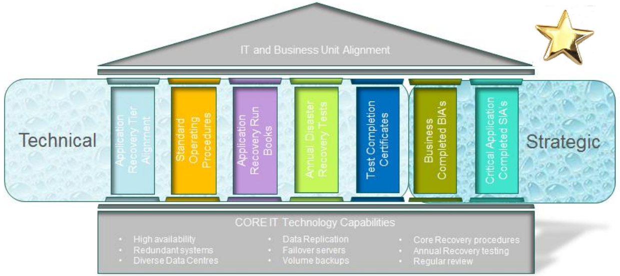
ICON IT Disaster Recovery Overview

ICON IT has Disaster Recovery Plans in place to recover all core technologies and critical business applications necessary to continue the business processes, the resources required to support them and the procedure to restore them if they are disrupted in any degree by any business interruption incident. The plans include details of all components listed in recovering the specific technology or application. The business interruption may be a direct result of a natural disaster, fire, terrorist attack, workplace violence, severe weather, and economic/political situations. The plans provide guidelines to ensure that needed personnel and resources are available for both disaster preparation and response and that, in the event of a business disruption, the proper steps will be carried out to permit the timely restoration of service.

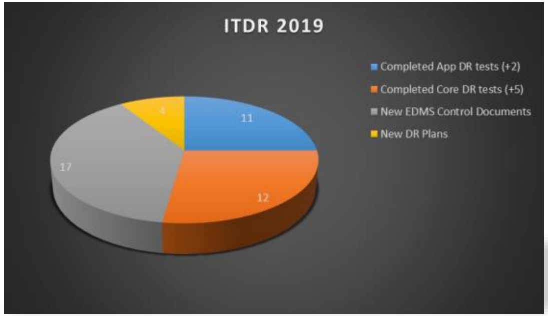
The Global IT Operations Team facilitates annual testing of the Disaster Recovery Plans by performing scheduled tests throughout the year and within an agreed timeline. The tests are designed to mimic an actual activation of the specific plan, measure activities against the committed RPO & RTO's, record success or failures, initiate follow up activities where necessary and to observe the response of the team members. Specific attention is given to the order and accuracy of recovery activities, ability of the team members to demonstrate an understanding of the overall recovery process, have a full understanding of all roles and responsibilities of the team participants, to independently determine the appropriate next steps, contact the appropriate people at the correct times, to make decisions as required, escalate issues as appropriate, and to coordinate the response of other team members, providing guidance and direction as necessary.

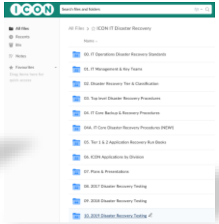
ICON Disaster Recovery SOP's

- IT113-SOP – IT Disaster Recovery Plan
- IT067-SOP – Data Backup & Recovery



IT and Business Unit Alignment
Technical
Application Recovery Tier Alignment
Standard Operating Procedures
Application Recovery Run Books
Annual Disaster Recovery Tests
Test Completion Certificates
Business Completed BIA's
Critical Application Completed SIA's
Strategic
CORE IT Technology Capabilities
• High availability
• Redundant systems
• Diverse Data Centres
• Data Replication
• Failover servers
• Volume backups
• Core Recovery procedures
• Annual Recovery testing
• Regular review



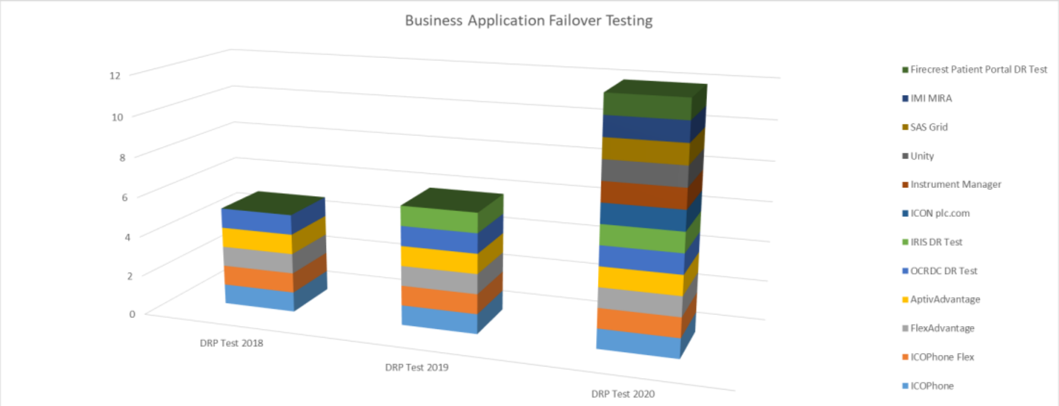


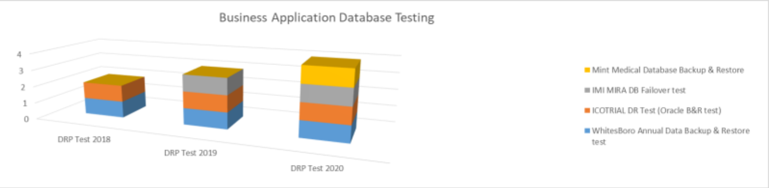
All Files > ICON IT Disaster Recovery

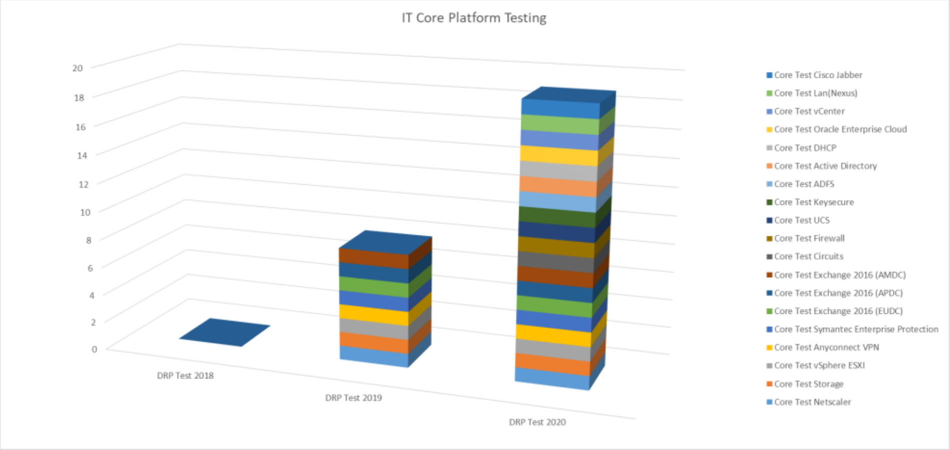
Name

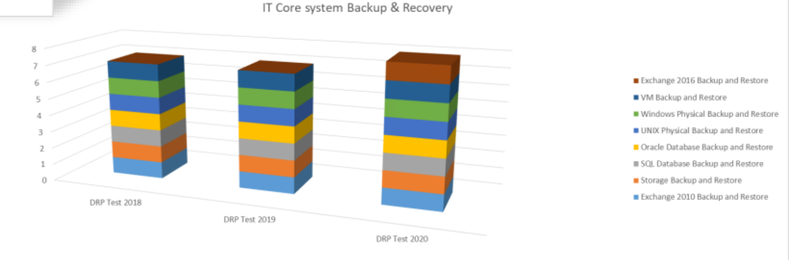
00. IT Operations Disaster Recovery Standards
01. IT Management & Key Teams
02. Disaster Recovery Tier & Classification
03. Top level Disaster Recovery Procedures
04. IT Core Backup & Recovery Procedures
04A. IT Core Disaster Recovery Procedures (NEW)
05. Tier 1 & 2 Application Recovery Run Books
06. ICON Applications by Division
07. Plans & Presentations
08. 2017 Disaster Recovery Testing
09. 2018 Disaster Recovery Testing
10. 2019 Disaster Recovery Testing

Disaster Recovery Testing Achievements









IT Operations – Disaster Recovery Achievements/ Activities 2020

Operational

Existing App test Queue
New App test Queue
IT Core testing
IT Backup & Restore
DRP Development

Compliance

MSB
Test Certs
SaaS Provider
EDMS M7
Audit

Standards

IT DRP
IT Position Statement
IT Backup & Recovery
IT Core tests
CMDB
ITDR Tier
DR Servers

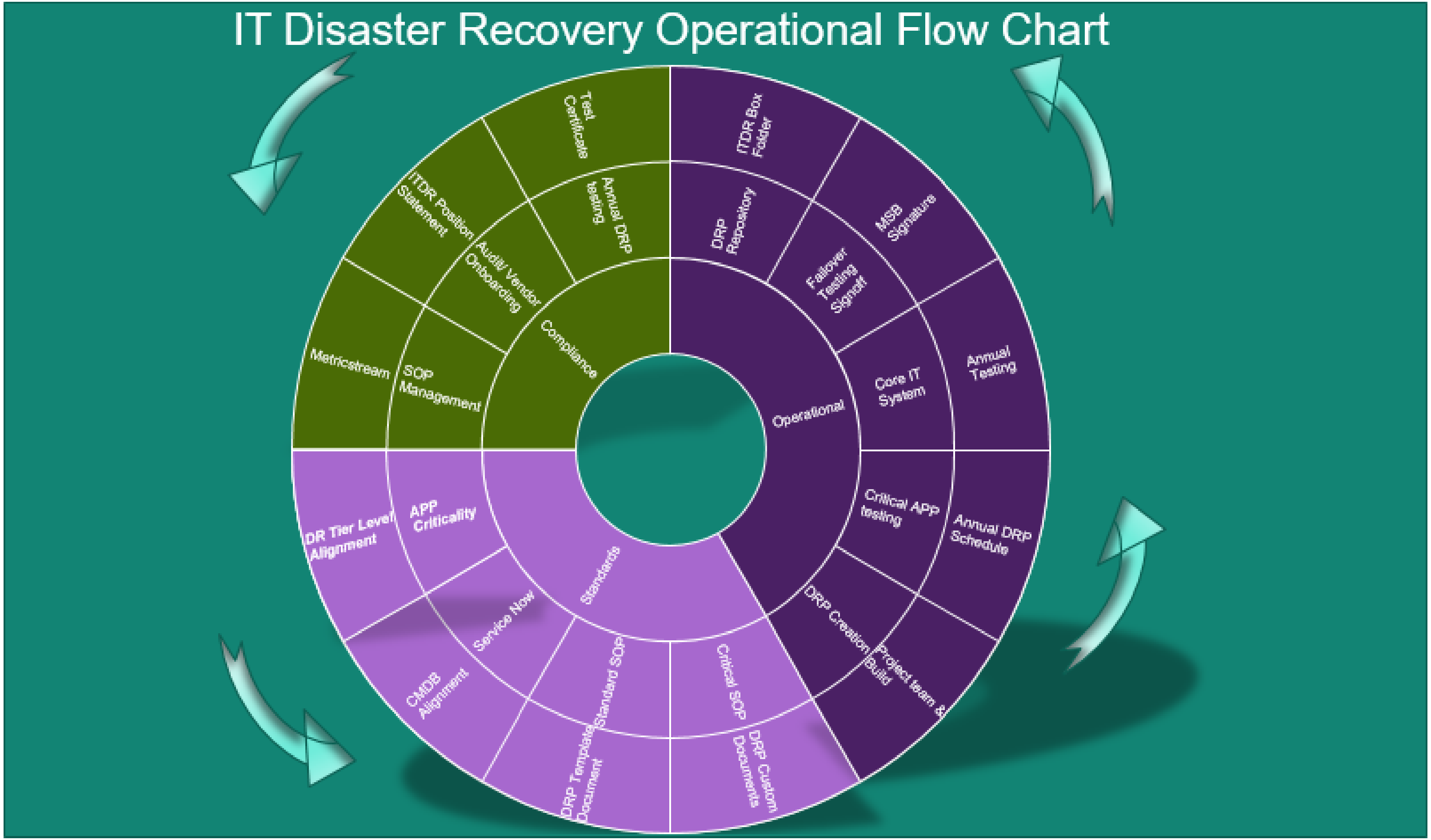
Strategy

ITDR
App Alignment
C2 BIA
Service Now
Playbook
RFI Support

Initiatives

ITDR Tech Roadmap
Digital Tx Alignment
Opex Savings
Project Foundry
Conference Speaking

Disaster Recovery Strategic Alignment



IT Disaster Recovery Playbook

ICON

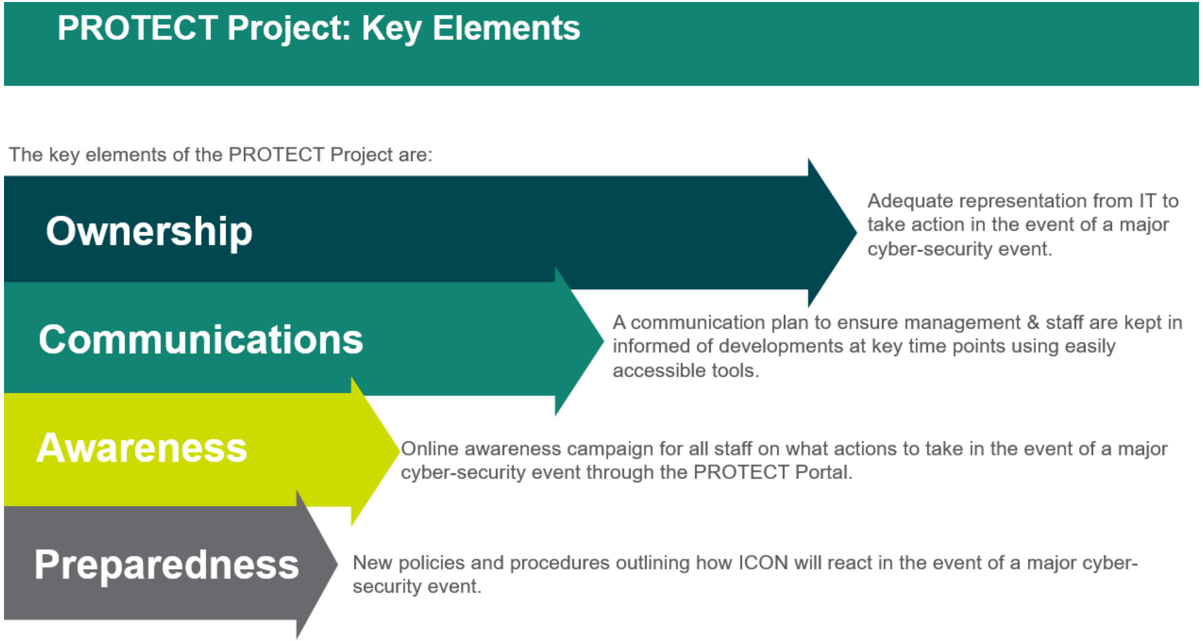
A Symbol of Excellence

IT Operations Play Book (People)

- Specific Plan for DR invocation
- Complete Contact List for all key IT Staff
- Complete Contact List for all key Suppliers
- Automated Contact List on mobile phones
- Specific Communications Bridge for DR invocation
- Technology ‘champions’ per platform
- Establishing Priority Activities list in a DR situation
- Recovery Sequence and Activities Management in a DR situation
- Annual Plan review

IT Operations Play Book elements

The four main elements of the Playbook are outlined below:



PROTECT Project: Key Elements

The key elements of the PROTECT Project are:

Ownership

Adequate representation from IT to take action in the event of a major cyber-security event.

Communications

A communication plan to ensure management & staff are kept in informed of developments at key time points using easily accessible tools.

Awareness

Online awareness campaign for all staff on what actions to take in the event of a major cyber-security event through the PROTECT Portal.

Preparedness

New policies and procedures outlining how ICON will react in the event of a major cyber-security event.

What is the Playbook

Activation – The Disaster Recovery Committee is responsible for launching the activation phase. As a member of this team, I am responsible for managing, coordinating, facilitating and interfacing with the IT Champions and Crisis Management team for the following:

Notification – by ‘Signal Text’, email – (external O365) and WebEx meetings. This will invoke the IT Crisis Management Team

Damage assessment - It could take IT Champions some time to assess the exact effects of the disaster. This damage evaluation should be executed as quickly as conditions permit, with personnel safety given highest priority. Only when the damage is assessed and the affected systems are identified can a recovery process begin.

Execution - The activities of this phase focus on bringing up the disaster recovery system(s). Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. Recovery procedures for specific systems & applications, which have been fully documented, will be referenced and can be obtained from an offsite repository with external user access for IT Champions **‘Box’**

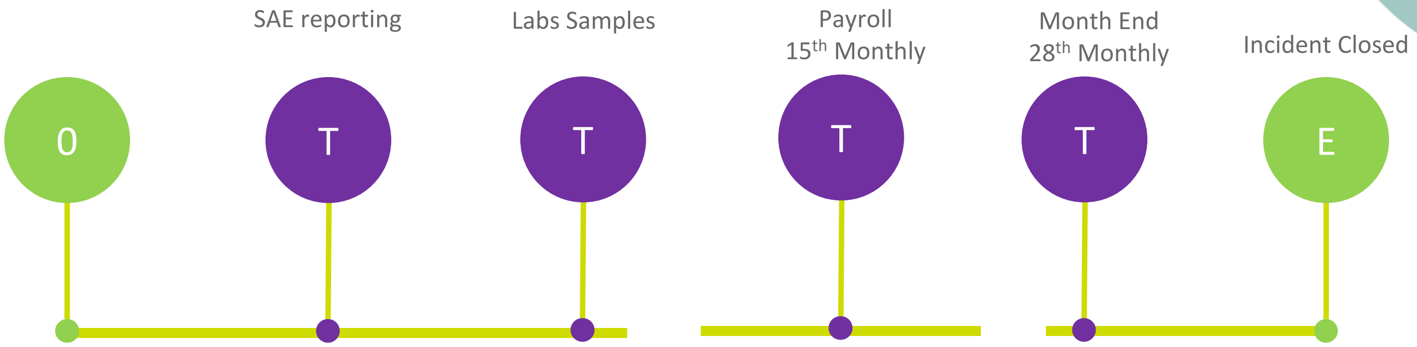
Reconstitution - In this phase, operations are transferred back to the original systems once they are free from the disaster after effects, and execution-phase activities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding and may take days, weeks, months to restore.

Communication is also a key component and role for me, throughout all phases by providing regular updates, from the initial + 0 hour to regular updates every 4 hours, to a final communication each day.

Tactical Recovery Phase - Time Dependencies

Are there any time dependencies, these may include:

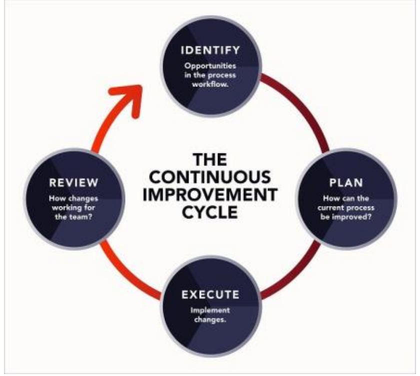
- Finance Process such as Payroll, Month End
- Regulatory Reporting
- Other time dependant activities important to your business



Continuous Improvement

Continuous improvement

- Continuous improvement is an ongoing activity that occurs at all points in the DR planning lifecycle, and can be implemented through effective programme management.
    - Periodic Reviews
    - Recovery Plan improvements
    - Automation opportunities
    - Separate Data Center Tenant configurations
    - Technology advancements
    - DRaaS in the Cloud (Azure/ AWS etc.)
    - Other


IDENTIFY
Opportunities in the process workflow.
PLAN
How can the current process be improved?
EXECUTE
Implement changes.
REVIEW
How changes working for the team?
THE CONTINUOUS IMPROVEMENT CYCLE

A Symbol of Excellence

William Doyle

Head of IT Disaster Recovery

Email:

William.doyle@iconplc.com

iconplc.com